eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Constructing and restraining the societies of surveillance:

Accountability, from the rise of intelligence services to the expansion of personal data networks in Spain and Brazil (1975-2020)

Jaseff Raziel Yauri-Miranda

Ph.D. Dissertation

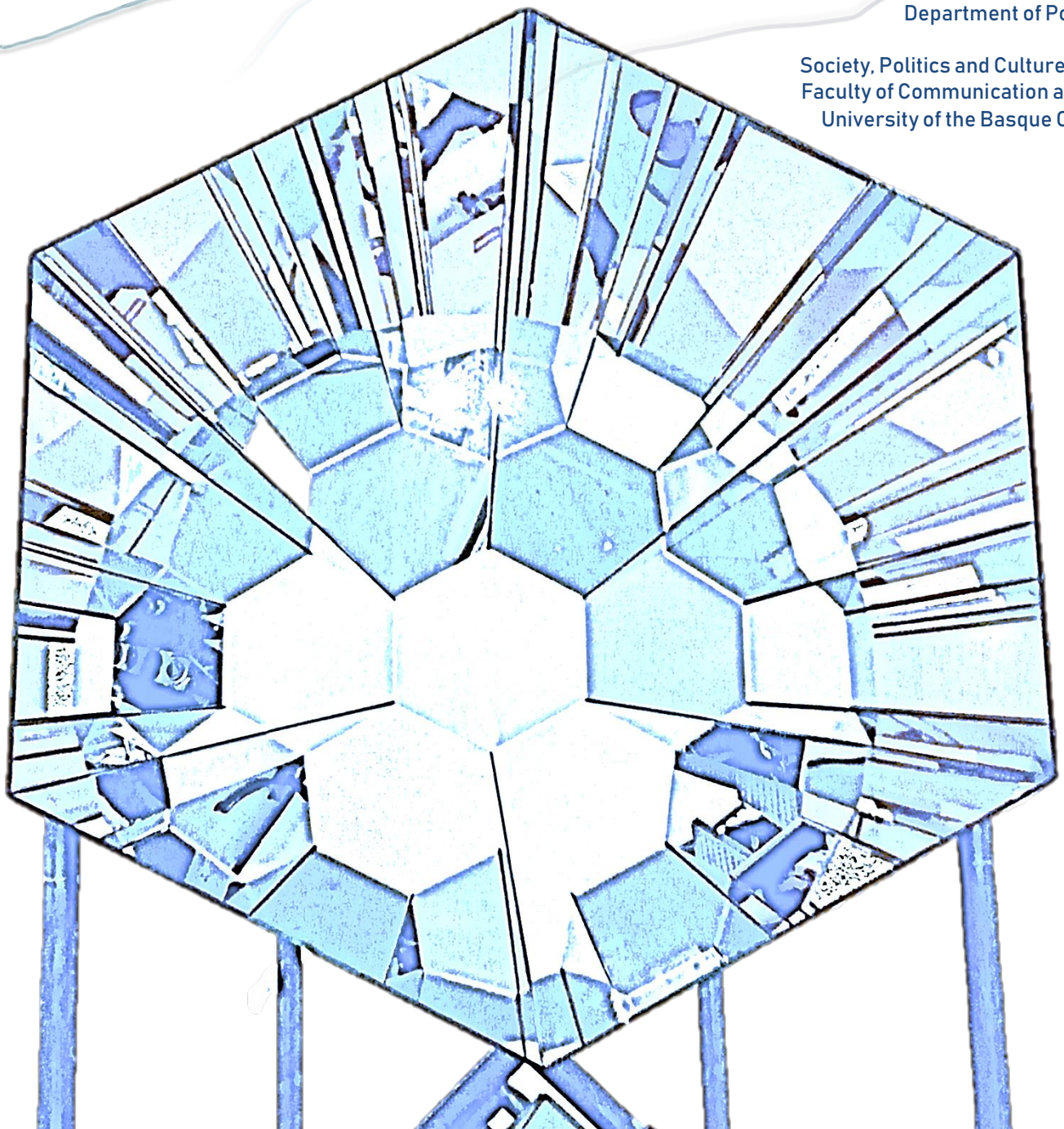
2021

[Construyendo y recalibrando las sociedades de vigilancia: Rendición de cuentas, desde el origen de los servicios de inteligencia hasta la expansión de las redes de datos personales en España y Brasil (1975-2020)]

Constructing and restraining the societies of surveillance

Jaseff Raziel Yauri-Miranda

Jaione Mondragón (Director)
Gema Martínez (Co-director)
Department of Political Science and Administration
Society, Politics and Culture Doctoral Program
Faculty of Communication and Social Sciences
University of the Basque Country (UPV/EHU)



Flectere si nequeo Superos, Acheronta movebo.

"If I cannot bend the will of Gods, I shall move Acheron and Hell."

Virgil. Aeneid, Book VII.

Abstract:

The objective of this study is to examine the development of socio-technical accountability mechanisms in order to: a) preserve and increase the autonomy of individuals subjected to surveillance and b) replenish the asymmetry of power between those who watch and those who are watched. To do so, we address two surveillance realms: intelligence services and personal data networks. The cases studied are Spain and Brazil, from the beginning of the political transitions in the 1970s (in the realm of intelligence), and from the expansion of Internet digital networks in the 1990s (in the realm of personal data) to the present time. The examination of accountability, thus, comprises a holistic evolution of institutions, regulations, market strategies, as well as resistance tactics. The conclusion summarizes the accountability mechanisms and proposes universal principles to improve the legitimacy of authority in surveillance and politics in a broad sense.

Keywords: surveillance, accountability, intelligence services, personal data, power

Resumen:

El objetivo de este estudio es examinar el desarrollo de mecanismos de rendición de cuentas (accountability) con el fin de: a) preservar y aumentar la autonomía de individuos sometidos a vigilancia y b) recalibrar la asimetría de poder entre vigilantes y vigilados. Para ello, abordamos dos ámbitos de la vigilancia: los servicios de inteligencia y las redes de datos personales. Los casos estudiados son España y Brasil, desde el inicio de las transiciones políticas en los años 70 (en el ámbito de la inteligencia), y desde la expansión de las redes digitales de Internet en los 90 (en el ámbito de los datos personales) hasta la actualidad. El examen de la rendición de cuentas, por lo tanto, comprende una evolución holística de instituciones, regulaciones, estrategias de mercado, así como de tácticas de resistencia. La conclusión resume los mecanismos de rendición de cuentas y propone principios universales para mejorar la legitimidad de la autoridad en la vigilancia y en la política de forma general.

Palabras clave: vigilancia, accountability, servicios de inteligencia, datos personales, poder.

Resumo:

O objetivo deste estudo é examinar o desenvolvimento de mecanismos de prestação de contas (accountability) com o fim de: a) preservar e aumentar a autonomia dos sujeitos submetidos à vigilância e b) calibrar a assimetria de poder entre vigiantes e vigiados. Para isso, abordamos dois domínios de vigilância: serviços de inteligência e redes de dados pessoais. Os casos estudados são a Espanha e o Brasil, desde o início das transições políticas nos anos 70 (no domínio da inteligência), e desde a expansão das redes digitais da Internet nos anos 90 (no domínio dos dados pessoais) até a atualidade. O exame da accountability, portanto, compreende uma evolução holística de instituições, regulamentos, estratégias de mercado, bem como táticas de resistência. A conclusão resume os mecanismos de accountability e propõe princípios universais para melhorar a legitimidade da autoridade na vigilância e na política em um sentido amplo.

Palavras-chave: vigilância, accountability, serviços de inteligência, dados pessoais, poder

Acknowledgments

(Agradecimientos)

A doctoral dissertation is not only an academic specialization and research analysis. It is also a story of life and continuous creation. It is not distant from craftsman work or making a film, writing a novel, composing a symphony, or inventing a dish. But, above all, it is the condensation of exploring and learning, meeting people, completing journeys, and remembering experiences. The pages in your hands were conceived during four lucky years in many places. From the shores of the Mediterranean Sea in Greece to the temperate forests in Canada. From the urban chaos in Samarkand to the lockdown and calm nights in Bilbao. From continuous reading and research to spontaneous insight and invention. In this task, I was supported by colleagues and friends in Spain and by the love of relatives in Brazil, Peru, Chile, the USA, Germany, and other countries.

I would like to thank the special orientation and comments of Jaione Mondragón and Gemma Varona Martínez, who were my directors and supported me academically and also trusted on me all the time. I appreciate the collaboration from professors and staff at the Department of Political Science and Administration (UPV/EHU). I also thank the comradeship of pre-doctoral colleagues like Alma, Eki, Eneko, Idoia, Uxue, and Aingeru. I am thankful to Priscila Brandao from the Federal University of Minas Gerais, who reviewed intelligence content related to Brazil, and to Antonio Díaz-Fernández, who helped me to write some intelligence parts from Spain. I am also thankful to Martha Michailidou from the Panteion University of Social and Political Sciences, who supervised my exchange program in Athens, and to John Nomikos from the Research Institute for European and American Studies. I am especially thankful to Minas Samatas from the University of Crete, who welcomed me on the sunny shores of this island, and to David Lyon from the Surveillance Studies Centre at Queen´s University, who received me in Canada with open arms and a bright soul. Both Samatas and Lyon were retiring from their respective centers and taught me academic and life lessons for the rest of my days. This work praises their humanist wisdom.

Despite the distance, I am grateful for the oceanic love of Julia and Jancker, es incommensurable mi ternura y aprecio, los quiero muchísimo. A Guido, que el destino te bendiga y te envíe mis abrazos y buenos recuerdos. Muchas gracias Mamá Julia y Mamá Bertha, mis corazones que aún laten lejos y que siempre me cuidaron. Gracias Ángel, Pier, Kristian, Mel, Mishell, Karina, Pepe, Norma, Zeida, Ederwin, Alex, Javier, Lili, Ricardo, Jimmy, esta tesis les rinde homenaje con mucho cariño y amor. Sin ustedes no sería nada.

My tremendous affection goes to amigos y compañeros de muchas curvas en la carretera doctoral como Miriam, chica fuego que me dio cobijo emocional muchas veces y de quien aprendí la fuerza de la superación. A Israel y Guille, mis caballeros

de muchas noches y bohemias, compañeros de la palabra y de la amistad procerosa. A Ana, cuya sensibilidad y principios mueven a uno y hacen que se disfrute siempre de buena compañía. A Eluska que, a pesar de los eclipses, siempre tengo recuerdos de su personalidad bondadosa y exquisita empatía. A Lara, quien tiene un corazón más grande que todos los salones de danza y teatros de toda la ciudad A Noemi, deseándole suerte en su aventura laboral al otro lado del mundo. A Raque y Kris que se convirtieron en mis mosqueteros y me hacen gastar el tiempo en buenas bobadas y charlas vitales. A Dafne que ha recurrido el océano y la península conmigo mostrando que la distancia no siempre es un obstáculo para el afecto. A Claudia, en sus andanzas y causas moradas. A Maider, Oráculo querido y que no se detiene en sus mudanzas. A Olga, Eva, Roque, Iker, Abdú y Azucena.

Salve minhas vadias do outro lado da pandemia. Despir Nefer, rainha blogueirinha e Karnal nosso. Botar o pau pra quebrar Douglas, que passou dos 27 raspando. Apostar em criptomoeda Nandinho, entregue a dissertação. Grande Gabi, mestre dos bares e dos gatos. Aloprado Thales, doidin no pô de prato e na psicanálise. Lindo Marcelo, inveja dos maridos na Ásia. Musical Lenine, na jornada tripla. Cavaleiro Hugo, com esquema no tráfico. Peculiar Julhelena, amante de plantas (recreativas). A antigas amizades com o pessoal da FAFICH, como Marco, Clone, Bruno, Cézar, Nathalia, Isadora, Mariana, Madsen, Xandao, Tamira, Raquel, Luísa, Alysson, Getúlio, Thiago Prates, Fabiana, Matheus, Lennon, Camila, entre outros.

To past good friends around the spherical world, like Midori, Tommy, Sachil, Rohit, and Nathalia. Greetings beloved Giova, Hannah, Stacy, Flavio, Braulio, Roya, Emma. The Northern life was more special with you all. To Elifcan, Anneka, Olympia, Rana, Elena, and old mates. The last part of this study reflects my appreciation and the time I spent in Hellenic lands. To Vincenzo, Ricardo, Yoly, and the Galician memories.

This work would have not been completed without the lovely support of Kathi and the Utxis. I am really thankful. May life show to you good roads. My gratitude also goes to those who shared special moments and now their paths, for different reasons, are distant such as Josu, Ane, Helena, and Yolanda. A velhos amigos do fundo da alma e que sobrevivem ao passar do tempo, Rolando, Webert, Bode, faço reverências a vocês. Al compañerismo de Eva, Itxaso, Ainoa, y Manolo. A la libertad de O´Connor, Ana, Abdesamad, Goldwin, Mohammed, y María Jesus. And to the kind love of Saioa, whose lips and soul resonate various frequencies on me. El viaje ha llegado al final de su trayectoria. Baina nire bizitzan bide berri bat ireki zenuen.

For the kind remembrance of Mr. Llerena who taught me the art of reading and writing during my childhood in the mountains.

Table of contents

List of figures

List of tables

Glossary of Terms

Accountability	Action or practice that restrains authority in order to increase legitimacy. It checks the forms, outputs, and allows validating a form of power. Accountability can be achieved through specific principles such as responsibility, answerability, enforcement, and transparency.
Agency	Capacity of the civil society to become an active actor. It consists of obtaining more power and autonomy. Do not mistake with the theory of agents and principals, in which agency relates to institutional representation and bureaucracy.
Algorithm	A sequence of steps and decisions to obtain a result. Commonly used in informatics to describe automated procedures to process certain data.
Answerability	This accountability principle relates to the capacity to demand "answers" and formulate corrections to another actor(s). It relates to restoring trust and correct wrongdoing.
Aporia	No solution or no way. A dead-end road to something.
Authority	Capacity to exercise power by soft and hard means. It hinges on *auctoritas* (prestige and tradition) and *potestas* (force and coercion) to influence, block, and even ignore another actor.
Biopolitics	Power over biological bodies. In surveillance, it relates to administrating a 'mass' of individuals in their biological and political constitution.
Commodification	To convert something into an economic or mercantile object. It can be used to describe the reification of the personal body, creativity, and data to reach monetization purposes.
Enforcement	This accountability principle relates to the capacity to impose sanction or hard correction to another actor. Justice and courts are traditional domains to enforce laws and guarantee fundamental citizen rights.
Exceptionality, Exceptionalism	The ability to create "new" politics. It is the generative dimension of power. It refers to foundational moments or deep alterations in the conditions that allow the exercise of authority.
Dataveillance	A form of surveillance conducted to collect, process, and use bulky amounts of digital data from individuals.
Differentiation	It is the process of becoming or constant transformation of an object. Also, it is the emergence of new social and technical fields. It can be compared to branches that stem from a trunk.
Governmentality	The techniques and the reasons to sustain politics and government. It is the generating dimension of power or the normal conditions that allow the sustainment and reproduction of authority.

Hegemonic	It refers to a powerful actor that dominates, by different means and purposes, other ones.
House of mirrors	Surveillance metaphor to describe the arrangements, procedures, and distortions of personal data digital flows.
Instrumentarian	Individuals turned into instruments by surveillance. Instead of violence directed at bodies, it operates like a taming or a sort of 'soft' totalitarianism.
Legitimacy	The ideal condition stemmed from the will of the people (i.e. the governed) that needs to encompass authority and power. It is the source that validates politics beyond legal rules and norms. Legitimacy can be expanded and improved through accountability.
Liberal, Liberalism	Political philosophy originated in the Enlightenment era that traditionally praises individual freedom and rationalism. Do not mistake with neoliberalism based on free market and with the term used to describe the USA political faction.
Metanarrative	Main narrative or thought in which political and historical actions converge to build common human actions. Traditionally, religions are examples of closed metanarratives.
Multitude	The heterogeneous and ever-changing groups of people. This sphere differentiates and even challenges other social domains like the state and the market.
Ontology, Ontologic	Relative to the essence and the specific meaning of something or someone. In philosophy, it explains the nature of being.
Panoptic, Panopticon	Surveillance metaphor that indicates visibility and self-discipline from the watchers upon the watched. It can be represented by a watchtower to surveille prisoners.
Power	Power is the potential capacity to influence other actors. In this text, we argue that it cannot be fully tamed; it has both exceptionality and governmentality features, and it entails asymmetries (domination and resistance).
Presentation	Accountability principle that expresses continuous participation and citizen involvement in politics. It transcends people as a sovereign actor in political and human dimensions.
Resistance	The capacity to challenge hegemonic forms of power. It relates to agency and multitude.
Responsibility	Accountability principle that indicates duties and missions owed or expected by one actor to another. It allows identifying the actors and the content of the accountable action.
Rhizome, Rhizomatic	A node or piece of a network with relative independence from the other parts. In botanic, it refers to plants that, if separated, each piece may be able to give rise to a new plant. In this text, it remits to the surveillant assemblage.
Security	A situation of predictability that allows governmentality. Security is the base to create and sustain any sociopolitical order. It has different connotations depending on its implementation and

	perspective.
Slides of visibility	A metaphor to indicate that transparency is not equally distributed among watchers and watched. It can be promoted or decreased on one of those sides, entailing modifications on surveillance means and goals.
Sovereignty	Traditionally, it was associated with state power and the ruler's ability to impose order. It also refers to the power to establish exceptionality and governmentality.
Surveillance	It is the continuous socio-technical interaction to collect, process, and use information from objects and individuals. This system ranges from the visibility and self-discipline of subjects to flexible networks that reproduce authority and power.
Surveillant Assemblage	Surveillance metaphor that indicates web formats or networks. Like rhizomes that spread across a field, the surveillant assemblage is decentralized, flexible, and a fluid apparatus.
Structure	The macro-political dimension or the 'general picture' in which social actors interact. It can be considered as the meta-agency level (the big battlefield scenario) to analyze power.
Teleology	In philosophical terms, it is the destination or goal of a human endeavor or political action.
Third dimension	Accountability actions that are conducted at the international level.
Utilitarian	It consists of reaching a goal despite the means. In ethics, utilitarianism valorizes the consequences above the forms.

PREFACE

Where is power, this must be controlled or tamed? Those who are powerful must be responsible and accountable to other people? If the reader answers positively, this work would help to deep into those questions. However, this work was also made to those people who do not agree with those statements. At least in practice since many people support those ideas but do not reflect the answers in their praxis. Hence, this work is a product of a doctoral dissertation but it also aims to show that even the reader has a role to redefine his/her position as a subject of power and as controller of power. In simple terms, we are not only witnesses in the construction of societies and history.

Throughout history, the life of individuals was decided by external factors, by fortune, and most of the time by the rule of autocrats or despots. Since the industrial revolution, extraordinary things have been achieved by science and technology to improve the lives of individuals. At the same, the world has experienced several attempts to improve social reality and defeat despotism. However, those attempts also appealed to forced coercion, mighty authority, and almost infinite power. The last century, acknowledged as the century of wars and revolutions, not only showed the scale of destruction but also the magnitude of human suffering. More recently, by the time of this writing, not only autocrats and despots have returned to rule entire countries, but the attempts to improve the social reality are discredited and political changes tend to focus on technological messianic salvation and individualistic solutions.

We have entered a century where the technological, social, and environmental dimensions overlap creating major challenges to communities and politics. In this precise moment, the world has "stopped" and one-third of humanity is confined to avoid more pandemic casualties. In this exceptional moment, new normality is being replenished, the mundane life of citizens is being changed. And the coming decades might see ecologic and deep social transformations. This is not the first time in history in which great changes happen. However, what is becoming loom is that some socio-technical fields are acquiring more capacity to shape exceptional and normal aspects in our lives. One of these fields is surveillance: the act of watching and being watched all the time. Surveillance redefines the notions of living, of individuality, of political opportunities, and future. Thus, if the challenge against tyranny, autocracy, and forced coercion has not disappeared, new battlefronts have been opened to fight for the very definition of normality and possible futures. The ability to shape normality is a tremendous, yet implicit form of power.

In that sense, this study wants to present two fronts or realms in which the very idea of the future and life of individuals can be redefined at a different scale.

The first one relates to the traditional dilemma to restrain the authority from exceptional organizations. It relates to the oversight and control of intelligence services in specific states after authoritarian periods and political transitions. The second one relates to the new dilemma to restrain power from normal organizations, in the sense that they might alter everyday life social interaction and communication. This realm relates to the governance of information that is extracted from individuals to administrate a certain population by using personal data. This is the case, for example, of search engines and social network companies.

In short, we focus on intelligence agencies and on personal data processors. In this analysis, many players, roles, and tactics emerge like in a game of power. Surveillance can be understood as a "serious" game and we have a role in it. Surveillance is also the story and the construction of the latest episodes of human history in the attempt to redress the complexity of reality and the possibilities to survive as autonomous individuals and as species. However, the paradox is that, the more we deploy tools and technical instruments to reduce that complexity, the more it seems we create entropy and ignore social dimensions to solve problems. History barely offers lessons from the past, and social sciences are not the medicine to cure social problems. Yet, those dimensions cannot be ignored to create and reshape new realities. In that sense, we focus on the political dimension, in the analysis of power –from institutions to ethics and resistance-, to examine the construction and the restraining of societies of surveillance.

In the political dimension, it is difficult to join the dots when it comes to analyzing the legacy of previous intelligence practices (such as the vigilance against students and workers), to elucidate the old dilemmas of security (such as the violent methods used to suppress political dissidents), and scrutinize the new role of secret services in the current interconnected and globalized world. It is also intricate to analyze the legacy of those practices in a time of digital technologies and social tensions (i.e. Internet of things, big data, mass surveillance, and heterogeneous demands from the multitude), as well as to promote legal reforms to regulate and process data flows used by international corporations and automated machines.

It is also a challenge to build a coherent narrative to link past events to prospective trends in surveillance that interplays with science-fiction and dystopian futures (from Orwellian realities of social control to Black Mirror scripts in which technology undermines humanity). In those examples, watching people can be legitimate and necessary. On the other hand, those actions might be conducted in the shadows and foster deviations of power. And if there is power, restraining tools and mechanisms to correct it should exist. Therefore, in this text, those and other examples of surveillance will be addressed through the lens of "who watch the watchers?" The pages below can be summarized as an extensive

(instead of exhaustive) attempt to turn accountable those who have a certain power to surveille and watch.

The idea of restraining power by institutional and legal mechanisms is historically recent. Assessing the quality and implementation of accountability mechanisms is even newer, especially in the field of intelligence as controls in this field emerged mainly after the 1990s. Even old democracies had their intelligence services unchecked by Parliaments and Courts until the recent past. In that sense, we must recognize that this research is historically conditioned. Adopting a critical perspective to assess intelligence practices would have been prohibited in the 1960s and 1970s in Spain and Brazil. Until the immediate democratic transition in those countries in the 1980s, this research probably would have been accused of disrupting the social order, questioning the national interest, or being ideologically biased just by inquiring the efficiency of security practices.

In addition, writing on surveillance, and by extension on intelligence and national security, was not a trending topic of scholars during the 1960s and 1970s, either because they were directly surveilled by the regimes or because writing and dialoguing with those who didn't dialogue was, most of the times, a dead end road. Those years were not easy, but even if this text offer recommendations for the transformation of security institutions in the present (their past mistakes and deviations must always be condemned), this research could have been labeled in previous times by some scholars as a vague attempt of correcting the incorrigible. In addition, some security practitioners might have labeled this work as the attempt made by an outsider to scrutinize an authority that must not be questioned or that "is not that bad". Yet, in our view, authority cannot be self-referential and always must be checked.

Nowadays, the same labels can exist but risks also come from a different nature. For instance, in the present, there is a constellation of discourses that must be taken into account to analyze and to publish surveillance studies. As surveillance logics have changed, now we live in a world where the watchers are plenty (from governments to companies and international players) and they have learned to take advantage of disruption, contestation and radical energy for governance purposes, rather than curtailing and suppressing these same energies. Moreover, official intelligence is not anymore a taboo as it has adopted other connotations beyond secrecy. The development of intelligence studies through an accountability approach is recent. Hence, it would be an anachronism to demand current accountability mechanisms to closed institutions in authoritarian periods. Yet, we assess the evolution and the directions of those mechanisms from the past to the present. Intelligence is not anymore a sacred and completely opaque domain. However, some colleagues have mentioned that accountability has several limitations to tame power, especially in closed policies. We agree with them until a certain point, but we also affirm that the strength of this practice is found in its

limitations and promises. It is important to control even actions that seem uncontrollable, as expressed in the first part of this research. And if closed domains and high-policies can be tamed or redefined, then there is potential room to create new realities in the politics of tomorrow, even in distant futures,

Despite being a study guided by a power perspective, this text draws from other disciplines and is oriented to general people and citizens worldwide. This study is the product of the commitment to the study of History and Political Science, the fields in which the author developed his academic formation. However, the research supports an interdisciplinary convergence to produce holistic and coherent knowledge that should be of interest to the mentioned fields plus Sociology, Philosophy, Law, Criminology, Psychology, Journalism, Social Movements, Economy, Cultural studies, Literature and Narrative studies, Arts and Aesthetics, Natural Sciences, Computing Science, Informatics Engineering, and other ones. At different stages of this work, those fields have redefined the writing, the theoretical ideas, the methodologies, and the objects for analysis. We hope this work can foster connections among historical, political, moral, cultural, cognitive, and technical fields related to surveillance studies and beyond. Moreover, this work aims to be useful to practitioners and non-practitioners in each field, as well as to intelligence professionals and personal data managers. In that sense, we would like to invite every person to participate in this "journey" to reevaluate our condition as watchers or watched in surveillance societies.

INTRODUCTION

In contemporary societies, many tools and practices have been constructed to facilitate the management of resources, information, and people. One of those fields regards to surveillance. Surveillance consists of watching and being watched. Many scholars affirm that the ways to construct surveillance entail visibility, representation, meaning, and material opportunities to people. In this work, surveillance is consonant with those statements but it goes beyond. Surveillance also entails relations of power and resistance. Surveillance is defined as the extraction and use of individuals' information for the management of populations and the production of biopolitics (biological and political subjects of power). Surveillance also encompasses the redefinition of individualities and the meaning of social reality. This is not saying that surveyors manipulate reality or certain players control everything and everybody. Surveillance is not only a rational action conducted by certain social actors. It is a social system that differentiates from other systems (security, education, labor, science, economy, etc.), yet, it overlaps and affects these. Thus, surveillance cannot be reduced to concrete players but naturally, they matter. In that sense, surveillance can be analyzed by focusing on key players in specific domains or realms.

In light of the above, we address two realms that are crucial to the construction and differentiation of surveillance. The first one relates to intelligence services and the second one relates to personal data networks. Those realms are explained because intelligence refers traditionally to high-politics (exceptional politics to the service of states) whereas personal data (the information of individuals on the Web) refers to normal politics or mundane practices conducted to live in society. Both realms regard to the collection, extraction, process, refinement, and use of information to construct knowledge and deploy techniques of administration (of people).

Both realms evidence the construction of surveillance societies. They show that new forms of power are being constructed in the last decades. However, if power is being constructed, it is also necessary to control it or turn power accountable. It is essential to restrain and redefine the execution and use of surveillance in both fields. In that sense, the objective of this study is to examine the development of accountability mechanisms in those realms in order to:

a) Preserve and increase the autonomy of individuals subjected to surveillance,

b) Replenish the asymmetry of power between those who watch and those who are watched.

The point “a” is understood as a basic precondition to enhance any idea of active citizenship in a certain sociopolitical order. It is the capacity to act as an individual, a sovereign person, in surveillance contexts that can erode not only privacy but also individuality. The point “b” is understood to reprogram the relationship between authority (the ability to exercise power) and legitimacy (the ground to sustain power). This point regards to replenish the increasing political distance between those who watch and are watched, redefining their tension and power. Naturally, there are many organizations and people who watch. Yet, in both realms, we focus on powerful actors that have more capacity to watch and process information from individuals, i.e. intelligence services and personal data corporations.

As mentioned, power must be restrained and become accountable, but why? Accountability offers an answer because it is a basic mechanism that serves to rethink and verify the outputs of power. It acts as a connector between authority and legitimacy. In this study, accountability restrains a specific form of authority, the capacity to exercise power, to produce legitimacy, the social and ethical dimension that sustains power. Legitimacy is the ground in which citizens authorize authority. It is the substance that validates power to be conducted. Authority and power can be exercised without legitimacy. However, self-referential authority and unchecked power would lack the social sustainment obtained by a legitimate power. The basic idea of accountability implies to enlarge the legitimate base that enlarges power and hinges on the “will of the people”. Despite being abstract, diffuse, and even contradictory, the voices from the people are the main source of legitimacy and every accountable action should be directed to them. Since people are the authors and receivers of governing actions, they are the “imperfect” base that enhances a more legitimate base to authority.

To assess accountability, we analyze several principles such as responsibility, transparency, answerability, and enforcement. However, historical contingency and constraints factors can affect the performance and the presence of those principles. For instance, transparency from intelligence agencies is scarce and difficult to be assessed most of the time. Yet, other principles such as responsibility can be promoted in this realm. Besides, the mere presence of those principles does not define a good or a bad account. Of course, the presence of only one of those components implies poor accountability performance. Thus, the key point consists in assessing the presence and the quality of those principles in concrete places and times.

In that sense, we focus on two sociopolitical orders: Spain and Brazil since the end of authoritarian regimes. The author of the study has researched and worked in both countries, owning a certain expertise and potential to formulate situated knowledge and to conduct an immersive cultural and social study. However, the selection is mainly explained because both countries have a

controlled difference that allow their juxtaposition and contrast in a case study approach. For instance, both countries are deemed as cases of slow, secure, and incremental transition into a more democratic scenario, especially in Europe and Latin America. Yet, they can offer clues to more countries and cases in the world as it becomes more interconnected.

In the first realm of intelligence, we start in 1975, after the death of Francisco Franco, the Spanish Caudillo, and one year after the beginning of the distention process initiated by the Brazilian military regime. Those years represent the authoritarian legacy in both countries and constitute the initial conditions upon which intelligence agencies were created or upgraded. In the first realm, we analyze and assess the emergence of accountability mechanisms to tame intelligence since the implementation of the first internal controls in the 1970s, to the latter institutional reforms in the 21st century. In the second realm related to personal data, we assess the accountability mechanisms that have emerged in the governance of personal data since the popularization of the Internet and the enactment of the first protection rules in Spain in 1992. The expansion of dataveillance (digital data+surveillance), data business, and the forms to resist to that governance are also covered in the last decades. The final year is 2020 as it represents the end of the study and coincidentally constitutes a critical mark in terms of biopolitics and surveillance due to the pandemic crisis. As the analyzed phenomena and the accountability mechanisms continue to be performed after this date, the final part of this study, regarding the meta-narratives of resistance and the future of surveillance, is one attempt to analyze prospective developments. We know that this gesture is very risky and not common to scientific studies, yet, we reformulated overall principles that we believe should guide the evolution of surveillance and general politics in the coming times.

In light of the above, the main characteristics or the study are represented as follows:

Main objectives:	To assess the evolution of accountability mechanisms in surveillance in order to: - Analyze the management of populations and individuals autonomy subjected to surveillance. - Redefine the asymmetries of power between those who watch and those who are watched.
Accountability core definition	It is the connector of authority (capacity to conduct power) and legitimacy (ground to sustain power).
Principles to assess accountability:	Responsibility, answerability, transparency, and enforcement (see Chapter 1)
Realms:	Intelligence (1), and personal data (2)
Research methodology: (See Chapter 2)	Case study research, aggregated perspective for a single unit of analysis (intelligence agencies in Realm 1), Governance Network analysis, holistic perspective for

	different units of analysis (state, market, and people in Realm 2).
Geographic scope:	Spain and Brazil
Time framework:	1975-2020

Regarding the structure, this dissertation has four parts.

Part 1 relates to the theoretical framework and the methodology. Chapter 1 examines the theoretical forms to interpret and deploy power, from institutions to people. The forms here addressed are restraining power, executing power, justifying power, and constructing power. The first form analyzes whether is possible to control or tame power. The second form examines the manners to execute power, via exceptional rules and normalized actions, in a certain place and time. The third form depicts a brief epistemological history to understand where power is located and how it justifies its actions. Lastly, the fourth form analyzes security, the initial issue that sustains power in the current political systems. In sequence, we address the main concepts and principles related to surveillance (such as the panoptic and the rhizomatic assemblage), privacy, and accountability. Chapter 2 exhibits the methodology and operationalization to assess accountability explaining the time framework (1975-2020), the cases (Spain and Brazil), and the division in two realms (intelligence and personal data).

Part 2 covers accountability in the realm of intelligence. Here, Chapter 3 analyzes the theory and concepts of strategic intelligence related to internal security. After the analysis of intelligence and the authoritarian legacies of this activity in Spain and Brazil, we turn to the institutional evolution of intelligence agencies in both countries. This is the most extensive chapter as, in sequence, we assess different mechanisms of accountability in this realm: internal control, legislative control, judicial control, international oversight, and the role of the media and society. Thus, this chapter covers the accountability of intelligence agencies from different angles, roles, and times. Chapter 4 reconsiders the main ideas of surveillance and intelligence to build intersections or connection points. These points regard to the surveillance metaphors (the panoptic and the rhizomatic assemblage) being incorporated in the realm of intelligence, to the operationalization of intelligence to manage subjects and populations, and we start thinking in further forms of intelligence accountability and new forms of legitimate resistance.

Part 3 covers accountability in the realm of personal data. Here, Chapter 5 formulates the basic notions to understand and process personal data in digital flows and networks. Then, we examine the accountability mechanisms considering the governance of personal data in three domains: state regulations, market strategies, and civic agency. State regulations refer to the evolution of the legal framework to oversee the management and collection of personal data by an array

of organizations, local and international, in Spain and Brazil. Market strategies regard to internet and data business, the main forms of accountability from big market players (such as Facebook and Google), and further approaches such as accountability of algorithms, privacy by design, and even the issue of oligopolies of data players in the global economy. Finally, the civic agency addresses those strategies and tactics from the multitude of people to challenge surveillance and the sociopolitical order in a broad sense, from rhetorical and technical tactics to massive protests. Chapter 6 builds intersection or connection points between surveillance and the governance of personal data. These points are the incorporation of the surveillance metaphors from the theoretical framework to the realm of personal data, the use of personal data to the management of subjects and populations in terms of biopolitics (power over a mass of bodies), and new forms of resistance and accountability beyond the civic agency strategies.

Part 4, *Postscript on the societies of surveillance*, is a sort of amending work inspired in the *Postscript on the societies of control* by Gilles Deleuze (1994) that in turn dialogues with Foucault (1975)'s *Discipline and Punish*. Yet, rather than focusing on the forms of control and surveillance, we finish our analysis by reconsidering resistance and the potentials of the civic agency. In that sense, this part exposes the importance of metanarratives to orient resistance and alternative forms to construct politics. Metanarratives are the major stories that orient history and humanity. Taking into account global ethics and the convergence of social and environmental crises, from local to international governance, not only metanarratives seem to be necessary today, but they also appear as necessary alternatives to support and connect social changes. We propose the construction of a metanarrative based on Legitimacy and Humanity to orient the quest for new realities, from feasible actions to those that belong to the domain of dreams. Based on those ideas, we revisit accountability and expand this concept to radical principles of representation, consultation, participation, and "presentation". We close the study giving concrete examples of how those principles can be mobilized again in the realm of intelligence and personal data.

This work covers almost five decades of profound social and technological changes. We believe that the contrast between exceptional aspects from intelligence and the normal or mundane aspects from personal data offers a broad landscape regarding surveillance. Furthermore, by using concrete epistemological contributions and methodological perspectives from different fields, we praise for interdisciplinary and holistic knowledge (Bal & Marx-MacDonald, 2002). Thus, the dissertation does not focus on a single object or seeks for strict causality relations. This text is an attempt to join the dots, to build a big picture from fields that tend to appear disconnected. Rather than being exhaustive, we aimed to be extensive covering different disciplines to rethink accountability in current societies. Therefore, the selection of topics was difficult and one limitation is that many objects and issues were left behind (see methodology in Chapter 2).

For example, police intelligence as well as personal data in the domain of security agencies were not directly addressed. However, we introduced some connections with these domains in the judicial control of intelligence and in the analysis of market players that process personal data. Another topic not deepened is the technical aspects that sustain many practices to process data. Nevertheless, those issues were mentioned on the accountability of market players in Chapter 5. Another topic that was not deeply covered is the increasing surveillance based on face recognition and other biometric instruments. In popular culture, surveillance tends to be associated with cameras and video-recording. Those issues escape from our objectives but they were partially addressed in the regulation and protection of personal data also in Chapter 5. Another issue is the role of crime to influence both watchers and watched. Indeed, this issue is mentioned as a form of disgusting politics. Yet, the links between criminality and surveillance surely deserve more attention in further studies.

A limit in terms of methodology relates to secrecy and classified information protected by law. This is the case of intelligence, in which we focused on open sources. As we analyze accountability through many perspectives, from institutional documents to media articles and leaks, we hope to counteract secrecy to a certain extent. Yet, secrecy also inhibits the use of interviews and surveys from practitioners. This methodology was left behind even in the analysis of personal data networks. The decision is explained because we adopt a longitudinal or historic dimension to verify the evolution of politics. In order to cover changing actors during several decades, it would have been necessary to collect a vast volume of interviews and surveys in two distant countries. This task was simply beyond the material capabilities of the research.

Another limit is that we might not deep into the full variables that affect individuals under surveillance. For example, the analysis might dilute variables like race, gender, sex, nationality, education, labor, accessibility, etc. However, when we speak of legitimacy from the people, we know that neither all the people live under the same condition nor are they located on the same ground to reach individual autonomy and emanate legitimacy. Thus, to cover those differences, in the governance of data, we offer a division that is representative of society: state, market, and the multitude. Again, this division might simplify actors and reduce the variables that affect them. But this division allows us to see big power distances, especially between watchers and watched -which is one of the dissertation objectives-. For example, our division allows verifying the power distance between big data processors that constitute the first economic force in the global economy and the multitude that use specific strategies to defy surveillance. In other words, rather than mapping all the variables and the whole plurality of actors, our division reveals representative domains of society and big power asymmetries that entail forms of domination and resistance.

Regarding intelligence experts and practitioners, we understand that this practice has many domains and fronts. Hence, when we mention the word intelligence, most of the time we refer to the strategic intelligence attached to the Executive with the mission to refine and disseminate information for the security of the state and society. Intelligence, as well as surveillance, is not necessarily evil or pathological. Yet, indeed there is potential room to commit abuses of power, wrongdoing, and unaccountable actions in this realm. Even in practice, there is potential room to mistake intelligence for the state with intelligence for the government. Moreover, we face intelligence and surveillance from a critical perspective, assessing their mechanisms of accountability, formulating recommendations, and thinking in new forms to turn those services more legitimate (see Part 2 and Part 4). In that sense, we aimed to build a critical examination and a constructive evaluation throughout the entire study.

Despite being an academic dissertation, this text addresses overall readers, not only scholars and practitioners. Thus, it includes a glossary of terms that can be consulted at any time by the reader (see page 10). These terms are deeply explained throughout the dissertation.

This work is composed of parts, which in turn are composed of chapters, and these are composed of sections. One can read this text in many forms. Aside from the linear and progressive reading, it is possible to read the four parts in random order as they are like 'rhizomes' with relative independence. In any case, the rhizomes join in the last Part 4 that condenses the ideas of surveillance, resistance, accountability, and politics in a broad sense and beyond our cases.

Another form is the quick reading. In this case, the reader can jump into the main ideas of each section. Those shortcuts start after the sign ***Epilogue*** and reformulate the main content in many sections. Also, there are tables that summarize the content of the parts in the ending pages. The quicker reader can even jump to the conclusion as this section exhibits the results and summarizes the four parts of the study.

PART 1

Chapter 1. Theoretical Framework

As surveillance in this research is based on a power analysis, before addressing the main topics of the dissertation it is essential to understand the very nature of power. Hence, first section in this chapter examines four theoretical forms to interpret and deploy power, from institutions to people. These forms are: a) restraining power, b) executing power, c) justifying power, and d) constructing power.

The first form analyzes whether is possible to control or tame power (and abuses of power). The second form examines the ways to execute power, from exceptional procedures to normalized actions in a certain place and time. The third form depicts a brief epistemological history to understand where power is located and how it justifies actions. Lastly, the fourth form analyzes security, the initial issue that sustains power in political systems.

Instead of historicize and establish a fixed definition of power, this term is covered through an interdisciplinary analysis to reveal its many dimensions. That is, there is no single theory of power and unique field to reveal it. For example, in the first form, the Chapter starts from aesthetics to see the limits of power, trying to grasp it beyond rational and programmed norms. It addresses a less explored perspective by social sciences as aesthetics perceives power as a channel of affections and sensations that mobilize social actors. Every power transformation also hinges on the tension between beauty and disgust. In turn, the second form draws especially from philosophy to explore the creation of power and the maintenance of power. This form introduces and confronts notions of exceptionality and normality, dismantling utilitarian approaches to execute power. The third form is based on history to understand the evolution and justification of power. Meanwhile, the fourth form stems mainly from sociology to analyze the construction of power considering security as the cornerstone of any sociopolitical order.

Considering the forms of power in section 1.1, in sequence, we use them to formulate the main concepts regarding surveillance (section 1.2), privacy (section 1.3), and accountability (section 1.4). Those concepts, in turn, will sustain the methodology and the examination of the case studies in the following Chapters of the study.

The reader can consult Table 1 in the final page of this Chapter to see the theoretical framework in a glimpse.

1.1. On the forms of power

1.1.a. Restraining power: About the importance of controlling the uncontrollable.

Who are these? Why sit they here in twilight?
- These are men whose minds the Dead have ravished.
Memory fingers in their hair of murders,
Multitudinous murders they once witnessed.
Wading sloughs of flesh these helpless wander,
Treading blood from lungs that had loved laughter.
Always they must see these things and hear them,
Batter of guns and shatter of flying muscles,
Carnage incomparable, and human squander,
Rucked too thick for these men's extrication.
(Wilfred Owen, Mental Cases*, 1717).*

Restraining political power could be easier if we consider abstract discourses rather than real politics. From authoritarian regimes to deficient democracies, formal democracies, and good democracies, the lack of accountability could facilitate corruption, abuse of power, financial crimes, conflicts of interest, political clientelism, and other problems. However, even in the realm of abstract politics, accountability neither appears spontaneously nor represents a catch-all solution for the mentioned problems. Evil doing seems to be part of everyday social life and is extremely difficult to be counter-balanced by "good" practices, let alone to be eliminated. It seems that the best accountability institutional designs and arguments cannot be constructed in the same magnitude and philosophical logic than abject practices. That is, if good and evil politics are dialectical sides of the same coin and are not detached from real politics, the former might have a different nature and perhaps a limited potential to promote effective social transformations. It is very difficult to implement good political standards and foster civic virtues in a certain place during several decades. But this same effort could be easily obliterated in a short period by hundreds of circumstances and reasons. Destroying seems easier than constructing. This is not saying that evildoers are stronger or are in more quantity. It means that evil, disastrous and pernicious practices might not be the symmetrical opposite of goodness and beauty. They might have a different logic that cannot be counter-balanced just by placing good intentions to pursue a certain political goal.

To understand the different between evil and goodness in political actions including surveillance, as starting point, we shed light upon this issue with aesthetic terms. In the last decades, political theory has experienced a sequence

from emancipatory perspectives, to vanguard intellectualities, deconstruction analysis, cultural studies, and identity movements. After this sequence, it seems that politics has been reduced to a struggle between those who argue that theory cannot really represent a certain object (de-constructionists) and those who still manage concepts as they truly "represent" objects from the real world (cultural and identity studies). That is, discourses and practices in politics, at least epistemologically, have been jeopardized by the (im)possibility to steer and digest their objects, and in turn offer clear solutions to social problems. It is not saying that problematizing objects prevent their representation or that political studies are obligated to offer simple and practical solutions. It means, as stated by Hans Gumbrecht, that in the face of the mentioned struggle, there is an alternative way to convince and orient audiences affected by severe social problems. This way is appealing to aesthetic dimensions such as the "presence", the capability to internalize and apprehend a certain issue by attributes such as beauty, sensibility, mentality, and ugliness (Gumbrecht, 2004).

Far from marketing strategies to deliver beautiful products, political studies must enter into the dimension of aesthetics to question and leave an important message to different audiences. Philosophers like Jacques Rancière affirm that the aesthetic dimension is the last place where politics were confined after the turns of political and artistic movements in the last century (Rancière, 2015). After radical social movements in the 60s and their absorption into disenchanted common discourses that are the opposite of their initial criticism, either as a product of contingency or as the transformation of the vanguard thought into nostalgic thinking, Jean-François Lyotard already identified "aesthetics" amidst the chaos of post-modernity as a privileged place in which the tradition of critical thinking can receive an orientation (Carroll, 1990). In other words, it is by aesthetical dimensions that politics may abandon a dramaturgy which consisted, on the one hand, in a plot in which people were actors of a linear narrative with a clear ending (emancipator and messianic ideologies) and, on the other hand, a tragedy performed by powerless subjects in a path with no ending and the repetition of the "End of History" represented by the hegemony of the de-regulated economy. If aesthetical terms can produce "meaning" or transform the place of the political, they need to be considered as a starting field to think on power.

In that sense, let us consider corruption, abuse of power, political clientelism, financial crimes, rampant violence, sexual abuse, racism and other sever problems as examples and typologies of *disgusting politics*. At the same time, let us consider institutional transparency, efficient accountability, public interest, social responsibility, racial and gender equality as horizons for *beautiful politics*. In the philosophy of aesthetics, beauty is more feasible to be represented, performed, and internalized by an external audience. On the other hand, disgust is more difficult to be represented as it has a component that cannot be fully appropriated by an external audience. This is because disgust, more than beauty, is related to

trauma or traumatic senses; feelings that can be represented as comparative allegories but not re-presented as aesthetical re-creations. As Virginia Woolf argues, trauma "is a zone of silence in the middle of every art" or something not able to be expressed in words. According to her, "nature and art will exist beyond human life and […] the bigger picture overrules personal suffering" (in Moran, 2007, p. 24). Individual and collective trauma is perhaps the most difficult experience to be retold and shared.

Sublime and beautiful feelings, on the contrary, facilitate communication and the re-presentation of internal experiences in a completer degree, even when they cannot be fully conveyed (Bennett, 2003). Beauty –from divine revelations to abstract ideas and humans actions- can spread the seeds of goodness. Moreover, beauty can treat the wounds of trauma and manage personal disgust. That is, disgust can be beautifully re-programmed and re-presented but it does not mean that disgust is beauty or something beautiful *per se*. The poem of Owen in the introduction of this section, for example, is an allegory of soldiers traumatized in a battle. The verses give an idea of their madness and confusion, but they are like veils or layers difficult to be transposed and so to understand their suffering. The aesthetical dimension gives an idea of the horribleness and the "presence" of war. Yet, trauma is refractory to logo-centric communication and appears fragmented in its externalization (Luckhurst, 2013). The wounds and suffering could be healed by replacing disgust with beauty, by the contingent and fading memory, or by using tropes of language and arts to solve its tension (Best & Robson, 2005). Yet, in those cases, disgust is covered by layers of beauty instead of being apprehended in its rawness.

Despite subjective interpretations, one audience can imagine the degree and nature of disgust but this cannot be internalized in the same degree and completeness as beauty. For Immanuel Kant,

> […] fury, disease, the devastation of war, etc., can be described as evil very beautifully, and even represented in paintings; but there is only one kind of ugliness that cannot be represented according to nature without ruining all aesthetic satisfaction and therefore all artistic beauty, it is the element which awakens disgust (Trías, (1982) 2011, p. 11).

Following this Kantian statement, one can retell the tragedies committed by surveillance and security institutions in the past; it is also possible to express the suffering of individuals in hands of torturers, the deliberated execution of political foes, the decomposition of kidnapped bodies that never will be found, the fear awoke by intrusive surveillance, the anxiety originated of pre-empted algorithms that sort and classify people, and the commodification of human creativity by technocratic tools. In short, someone can mention how disgusting politics is exercised by different methods and in different periods. For example, violence can

be narrated appealing to images and personal testimonies, but it only will serve as an attempt of apprehension rather than something that can be truly re-presented. For Kant, disgust cannot be really assimilated and breaks every beautiful aesthetic apprehension of the social reality. Moreover, the pace of time tends to erase its immediate understanding. Hence, disgust cannot be fully comprehended and totally counterbalanced even with the best arguments from the politics of beauty. In the real world, both beautiful and disgusting politics are intertwined when it comes to analyze and understand social practices. But whereas the former can be represented and incorporated to wake up new realities and foster political transformation, the latter can execute transformations without being fully represented and justified. For Oscar Wilde, "Only what is fine, and finely conceived, can feed Love. But anything will feed Hate". Thus, disgusting politics cannot be simply juxtaposed to beautiful politics with the hope to override evil. They do not share the same logic and magnitude. For Wilde, again, "[Love and Hate] cannot live together in [a] fair carven house" (Wilde, (1905) 2010, p. 76).

Disgusting politics will continue to be committed not because good men are incapable of deterring the banality of evil, as coined by Hannah Arendt. Evil will be committed because even if we are affected by evil actions, our answer and good intentions will be performed by a lesser understanding and imperfect assimilation of evil practices.

In a micro-social example, the execution of torture perpetrated by Spanish security forces upon a political dissident was written by Isaac Rosa in the novel *El Vano Ayer* (The Vain Yesterday, free translation). Despite being a fictional story, the author brought up literary mechanisms to reconstruct the experience of suffering torture. First, he quoted a manual of instructions of torture which was released by security officials in order to maximize the physical and mental pain to accelerate the collection of information. As this technique was insufficient to depict the experience of torture, Rosa used distinct figures of speech to narrate the intensity and the details of two sessions of torture, including psychological delirium, crushing bones and internal bleedings as completer images that described abuse of power in the Spanish Franco regime (Rosa Camacho, 2004). This type of narration is completer than vague statements such as "torture was a common practice", or "thousands of men and women were tortured" in those times. Literature narratives bring up the experience of trauma; yet, we still need to rethink the forms to restrain and counteract the banality of evil.

In a macro-social example, historians have tormented themselves questioning the better forms to retell traumatic events, such as the Holocaust, in order to promote historical memory on these episodes and to develop ethical values in the present. Notwithstanding, this kind of event is refractory to historiographic representation and aesthetic apprehension. We do not fully represent and understand them because we do not recognize their disgusting

horribleness; we either fail to admit the size of human horror or are incapable of give meaning to such terrible violence. In that sense, Fernando Garcia infers the human inability to recognize its potential for evil. Hence, to describe this kind of traumatic event, he argues that historians put this kind of experience as limit events of apprehension in which individuals who participated in might be represented as monsters or infra-human victims (Garcia, Vieira, & Mendes, 2014). Alternatively, recognizing the humanity of aggressors and victims is ethically important but it is aesthetically limited because "we" cannot be equalized to "them". Telling that "we" are like torturers or share the capacity of being evil like "them" might help to understand past events but this undermines historical specificity and the effort to construct ethics. After disgusting events, the bridge of alterity seems to be broken and the attempts to cross it are always a challenge.

Incapable of fully understand and really answer to traumatic and severe disgusting politics, our relation with evil is controversial. On the one hand, we are attracted by the attempts to understand it even when this promise will not be fulfilled. This attraction might cause mere curiosity to consume disgusting symbols. It also can produce vertigo at the imminence of feeling disgust, as in the case of some murderers who feel pleasure while they inflict pain to victims. The joy is the vertigo at the imminence of something they cannot understand. On the other hand, we divert our apprehension of disgusting politics using alternative tools, such as constructing humoristic narratives or simply escaping from the range of disgust. The latter reaction is crucial to understand why many people are not interested in hidden practices, such as surveillance and intelligence, as they prefer to ignore politics leading with disgusting elements that must remain buried. Sometimes, for them, the darkness of our governments should continue in the shadows. In that sense, beauty is the beginning of the disgusting continuum that we can still bear, to use terms of poet Rainer Marie Rilke. Moreover, disgust is a part that should have remained hidden but was revealed, as stated by Friedrich Schelling. In short, beauty and disgust maintain a dialectic relationship that escapes the simple contrast or juxtaposition of opposite forces.

Let us describe the dialectic relationship between both poles in a completer manner according to aesthetics propositions. According to Eugenio Trías, the first proposition is that beauty, without a relationship with ugliness and disgust is scarce in force and in vitality to be considered as beauty. The second proposition infers that, when disgust appears without a previous mediation or transformation (metaphorical or metonymic), it destroys the effect of beauty. Therefore, disgust can be considered as the limit of beauty. In the third and last proposition, beauty is always a veil through which chaos must be felt. Thus, disgusting elements are fetishistic, as they locate the audience in a position of vertigo, in which the subject is about to tell or see what cannot be told or seen. For this reason, the aesthetic, artistic, and even political representation of beauty works as a veil, a penultimate

position before the quasi revelation of disgust; a revelation that does not occur because of those propositions (Trías, (1982) 2011).

In a political allegory, beautiful and disgusting politics could maintain a similar dialectic. Whereas we can appreciate or promote the great value of beauty in politics (such as a deeper democratic culture and efficient accountability), this appreciation cannot be really done without the constant menace of disgust (such as the return of tyranny and the lack of civic virtues). Secondly, the latter erodes the apprehension and the effects of beauty as well as its promise for a better future. Deviations of power as well as other examples are the limits or borderlines that can destroy political beauty attempts. Thirdly, disgusting politics are always one position ahead of those of beauty. When both sides encounter each other, the latter works as a veil that cannot be transgressed as beauty cannot reach the core of disgust (otherwise it will be destroyed) and because disgusting politics cannot be rhetorically expressed and sociologically full revealed. Again, beauty and disgust are not just symmetrical opposite forces. These poles maintain a relationship that escapes from a zero-sum game as they constitute a dialectical logic with the preeminence of the latter.

In light of the above, beautiful politics and good practices, such as anti-corruption and accountability mechanisms, are limited by disgusting politics, such as corruption and abuses of power. A corrupt activity is per se the target and the limit of an anti-corruption attempt. The damage caused by corruption, when executed by disgusting means such as violence, cannot be completely retold, assimilated, or understood. Ultimately, this violence cannot be entirely covered by anti-corruption discourses and practices because they are like veils that cannot unveil the last layer of disgusting violence executed against someone. And if anti-corruption practices deploy disgusting means (like violent police that act with impunity) to counterbalance disgusting politics (like money laundering gained from human trafficking) the "good" intentions turn up emulating its anti-values, in this example, by creating more violence when combating violence. What is worse, those means turn up creating new sources (of violence) that expand the layers that cannot be unveiled and reached by good politics, such as anti-corruption ethics and good legislation.

The same could be said about the accountability of surveillance. If the former belongs to the realm of beauty against the disgusting effects of deviation of power, abuse of force, exclusionary discrimination, and other surveillance evils (even when it is handled with good intentions), then accountability is limited by surveillance and by the attempt to counteract those bedevils. We will address the characteristics of accountability and surveillance in the next sections, but the point now is that accountability, in this case, depends on surveillance to be politically "appreciated" and executed. Besides, accountability mechanisms are always one step behind surveillance because the former acts like a veil that will never reveal

and unmask the real surveillant assemblage, not only because of surveillance secrecy or due to the lack of accountability efficiency, but because the disgusting potential committed by surveillance practices are the "last" frontier that will be never reached.

If this is true, why accountability is necessary to oversee abuses and deviations of power? Is this a lost battle in *a priori* terms? To answer this, first, we need to remind that disgust will be executed by several political players regardless of the existence of beautiful intentions. Disgust, evil, and hate can be auto-referential practices or attached to "good" endings. Secondly, even if severe disgust stemmed from certain surveillance activities cannot be fully understood and addressed, accountability still works as an enhancer of the politics of beauty. Beautiful politics still could enhance more politics of beauty. There is no zero-sum-game between disgust and beauty; rather they might be interpreted in dialectical terms as mentioned above. If accountability has limitations and depends on its target, i.e. surveillance, the former always can be improved in several dimensions. Institutional oversight, budget control, law enforcement, societal ethics, and other mechanisms could be replenished as categories of beautiful politics that can nourish good changes in social reality. For instance, government, law, and enforcement institutions might pave the road to beautiful politics but only if they avoid disgusting methods. Otherwise, they will undermine the whole accountability effort. As in the anti-corruption allegory, the expansion of disgusting and abject means would expand the layers where accountability and beautiful politics cannot penetrate by good means. That is one reason that stands the importance of controlling the uncontrollable and why beautiful politics must pursue the sinister even if it is ultimately unreachable. A second reason comes from other characteristics attached to accountability: transparency to understand and process disgusting politics.

In multiple approaches, there are no doubts that power is executed also in an "obscure" dimension where the shadows allow discretional ability to create disgusting politics. The premise of secrecy, the *arcana imperii*, is not detached from the capability to produce and maintain a certain level of power. A priori, secrecy neither is negative nor is the result of "realism" in politics: the competition with other powers and the response to threats posed by political enemies. However, secrecy is a conscious solution and an unconscious dispositive that could cover disgust practices because politics without a level of secrecy is not politics. In the same logic of disgust, power needs and contains the last layer that cannot be revealed. At the imminence of being unveiled, and when it becomes totally transparent, it turns into something else except power. "Without a secret sphere, politics becomes corrupted into a theatrical form that can only be understood as a stage with spectators," says Byung-Chul Han. For the philosopher, "the more political a performance is, the more it covers up secrets" (Han, 2015, p. 46). Even when accountability is simplified into transparency which in turn can be

transposed to sincerity, it is permanently difficult to counterbalance and assess lies. For Vladimir Jankélévitch, "sincerity is valid only in an opaque world in which the consciences are not transparent to one another and in which sincerity introduces light into the folds, into the shadows of lies" (in Marques, 2017, p. 137). Ultimately, politics will never be completely detached from lies, secrets, and disgust. Far from fatalism, this is not disgusting *per se* but it is something that can be interpreted as disgusting. When power contains lies and mask secrets, they even can be beautifully represented. Yet, they continue to be lies and secrets that can affect real people and leave consequences. Aesthetics and ethics separate but also converge, especially in social domains. We will return to this tension in Part 4.

Ultimately, political actions embodying disgusting elements are unreachable limits for beautiful attempts such as anti-corruption, transparency, and accountability. The latter cannot be understood at the same level or as mere solutions to disgusting politics. Rather, they must be interpreted as restraining mechanisms that enhance other dimensions of beautiful politics, affecting and redirecting the execution of power in a dialectic form. And, at this point, one statement against the dialectic relationship between beautiful and disgusting politics could be related to the fact that the roads to beautiful endings might be permeated by disgusting methods worth trying. Radical energies and contestation are still political paths that are not closed to political experimentation even if the present has frozen past clashes and violent approaches. But we should be alert as disgusting politics appear many times disguised by beautiful methods and goals.

For example, anyone looking into the past is forced to find several examples where violence appears to be dissimulated. When war is the continuation of politics by other means as coined by Carl von Clausewitz, or when violence is the lubricant for economic development as in modern military affairs, those abject or disgusting values never appear as ending goals that show their completeness and full nature. Instead of being reveled, they are protected by layers of beauty. Without them, they cannot be performed and assimilated by an audience. Their full revelation would produce the mentioned fetishist effect of vertigo or repulsiveness.

In that sense, even language is modified in an attempt to describe or execute disgusting politics. The vocabulary used by the Nazis in their "Final Solution" and the invention of the term "genocide" suits this case (Lang, 1991; Barel et al., 2010). In addition, euphemisms help to describe that war is never the ending goal of warriors; it is a "last resource" to achieve the "irresoluble peace". Within that logic, military affairs prefer to use "aerial vehicle of accelerated response" to describe bombing drones, or "plant of manufacturing of tactical and defensive logistics" instead of "factory of missiles". During the Brazilian dictatorship, security officials were awarded the "Medal of the Peacemaker", an award traditionally given to those who contributed to bringing "stability" to the country. Years later, those

officials were accused by covering crimes against humanity and torture. That is, during the military regime, peace was achieved at the expense of disgusting methods.[1] Those examples show that disgusting actions are covered by layers of "beauty" even in language and in different times.

To reach beautiful ends, both beauty and disgusting means might overlap. However, considering the dialectic relationship shown above, even the justified and necessary disruptive transformation of social reality must burden with side effects transformed into new sources of disgust, of evil, that in turn could constitute new limits to beauty. Beautiful prospects are possible but they will ultimately never cover the last layer of disgusting politics aimed to be transformed. The beautiful part in this quest will be eliminated insofar abject politics are the limit that cannot be transposed, retold, and tamed. In that sense, alternative political paths neither will achieve "happy endings" as a permanent condition nor will counterbalance evil objects by appealing only to good practices. This is the dead-end for beautiful politics as they cannot cover the last layer of disgust, which is unreachable in dialectic terms but not in a historical perspective.

In dialectic terms, beautiful futures and utopic endings are eliminated as a final goal to be aimed. In historical terms, it does not mean that imperfect but better futures are possible, either by appealing to abject or beautiful means. If there is not a simple solution between those sides, the good news is that the limits presented by disgusting politics are constantly changing and can be altered according to the contingency and to the relationship with beauty; a tension that escapes the simple clash of contrary forces. In those changes, if evil cannot be fully tamed, at least it can be redirected. If this is the case, then, controlling something "uncontrollable" requires a continuous effort to manage the constant dialectic tension. That effort introduces the dimension of time as well as concepts related to exceptionality and normalization in politics.

1.1.b. Executing power: The aporia between exceptionality and normalization

In this work, we support a vision where certain political mechanisms, such as accountability, must be deployed to control and restrain the exercise of power. We can understand power as some entity, a dimension with the capacity to bond other players and redefine the social reality. Traditionally, in ancient and modern societies, power is a relationship of subordination, in which a group of people set the rules and others comply with them, in which decisions are made within a set of

[1] Alessi, G. (2019, March 29). Ditadura militar brasileira: Não me arrependo de nada. El País Brasil, Retrieved from https://brasil.elpais.com/brasil/2019/03/28/politica/1553789942_315053.html

rules that are obeyed and the acceptance is made in the consensus or by imposition. In short, it establishes the recognized and accepted relationship of subordination (Bobbio, 1987; Weber, 1978). Yet, when it comes to understanding power in a certain place and time, one of the main issues relates to the execution of sovereignty. That is, who decides, creates, and governs and in the name of what or to whom?

The problem of the execution of power, of sovereignty, goes further than the permission to represent or exercise the collective will. It goes beyond the act of governing, the government, the creation of rules, the commission of violence, the act of caring, the act of founding a sociopolitical order, or even starting a revolution. The problem of sovereignty is an amorphous and polysemic term but according to Regan Regan Burles, it presents a dual character: it is both generative and generating of political life. It is generative because sovereignty must be constructed upon some foundation, i.e. a limited space and a certain period, and it is generating because it needs to reproduce its conditions by appealing to the special generative moment and to everyday politics (Burles, 2016). In that sense, the problem of sovereignty is a problem of separation between its capacity to promote exceptional generative conditions and the ability to sustain itself in normal or continuous generating situations. Therefore, we must look for the relationship between exceptionality and normalization.

Sergei Prozorov reallocates the problem of sovereignty in a double spatial and temporal dimension. The generative characteristic of sovereignty is constructed in extraordinary temporal moments of foundation (such as rebellion, crisis, a new Constitution or an alternative government) and outside spatial objects (such as rules and individuals placed in the fringes and even outside the center of the sociopolitical order) (Prozorov, 2005). In the same logic, the generating characteristic of sovereignty is related to the normalization of the moments to govern every day and in internal spatial objects which comprises the sociopolitical order. In this view, exceptionality is spatially outside and temporally in the singular moment whereas normalization is spatially inside and temporally is routine.

Either in normalization or exceptionality, sovereignty shows its multifunctional characteristics that could be combined in deeper analysis. Didier Bigo's conception of the “banopticon” is a junction of strategies for surveillance and control marked by exceptional powers that become permanent. This kind of power excludes individuals based on profiling and categorizing. At the same time, it normalizes the non-excluded through the production of political imperatives for the sake of security. Thus, Bigo highlights how sovereign practices of inclusion/exclusion are enabled by governmental strategies and procedures. In another example, Jacqueline Best argues that finance global governance blurs the borderline between normalization and exceptional sovereignty not only because it

ignores and changes states jurisdictions but because it reinforces mutual sites of power between governments and financial elites to create exceptional decisions, such as avoiding the bankrupt of banks that were "too big to fail" in the economic crisis in 2008 (Bigo, 2008). Giorgio Agamben, meanwhile, infers the sovereignty capacity to ban or regulate unwanted lives as the epitome of sacred violence and authority visualized in special circumstances and places from the ancient Roman Empire to the modern concentration camp (Agamben, 1998). Those authors, hence, blur the distinction between exceptional and normal sovereignty power.

The combination and the increasing indistinctness between normalization and exceptionality have been transformed in the statement that "the exception is the new rule" especially in a period of War on Terror, economic crises, pandemic emergencies, and social convulsions. The exception has become an element of regular policies. Sovereignty takes place in times of emergency, but it also works throughout the dissemination of power observed every day. That is, while the line between them may be blurred, arguably it is extremely difficult to distinguish between exceptions that are produced by normalization, or normalization produced by exception. For this reason, exceptionality and normalization neither can be placed in a spatiotemporal dimension nor can be separated by a distinction zone or borderline (Burles, 2016). And the collapse of the distinction between normalization and exceptionality could be demonstrated by reconstructing the political thought about sovereignty.

In Michel Foucault, for instance, the famous claim that political theory must "cut off the King's head" means that sovereignty must be reallocated and analyzed beyond the power of official rulers and institutions. In *Society Must Be Defended*, *The Birth of Biopolitics*, and *Security, Territory, Population*, Michel Foucault stated a concern regarding the status of sovereignty and its relation to power in his description of *governmentality*. Governmentality is a genealogical inquiry that questions the bondaries of the political in everyday situations and beyond government actions and reasons. This reason, the mentality of government, affects and produces a new realm of thought called 'politics.' According to Foucault, governmentality does not simply imply force, law, and official discourse. It produces a new understanding of politics by amorphous and unconscious tools where the appearance, the attraction and the non-explicit dispositives are also important to elaborate a particular way of thinking and of programming the specificity of government in relation to sovereignty (Foucault, (1978) 1991). Politics here cannot be summarized to the relation between sovereign and subjects; rather it is the execution of discipline and management deployed across various social and political institutions (religious, medical, educational, military) that produce political order through processes of routinization and normalization. Normalization, as Foucault explains, does not divide normal and abnormal. Normalization for him is "a distribution of normality" in which the aim is "to reduce the most unfavorable, deviant normalities in relation to the normal, general

curve" (Foucault, (1978) 2007, pp. 60-62). In doing so, sovereignty is able to construct its generating component and auto-referential logic which sustains itself every day and in normal circumstances. In short, sovereignty is not a monolithic entity; rather it is comprised of dynamic forces and forms of subjugation that are dispersed and are not fully cohesive. Governmentality, meanwhile, can be related to "biopolitics" in order to manage subjects and populations. Foucault wrote that biopolitics consists of a set of rules, a political regime, that "exerts a positive influence in life, [with] endeavors to administer, optimize and multiply it, subjecting it to precise controls and comprehensive regulations". It is a situation where power is applied to the "function of administering life" (Foucault, (1979) 2008, pp. 137-138). In that sense, governmentality uses biopolitics to focus "on the body" as this entity serves to biological and political processes: "reproduction, birth, mortality, health, life expectancy, longevity and all the conditions that regulate them" (ibid.: 139).

On the other hand, for Carl Schmitt, the domain of the political can trace its foundations to the original decision on who is the enemy. In *The Concept of the Political* and *Political Theology,* he argues that the binary distinction between friend/enemy is the first political act, the criterion by which all other political fields are determined such as morality, arts, and economics. This initial decision is exceptional and is something reserved to the sovereign, and it is by this ability that the sovereign is acknowledged. Schmitt is concerned in the foundation or generative moment rather than in the everyday mechanisms of the administration of government (Schmitt, (1932) 1976). The friend/enemy distinction mark routine practices, but these are secondary forms of politics that are not connected to the essence of the political, the truly sovereignty characteristic is attached to the foundation, to decide the "us" and "them" (Schmitt, (1934) 2008).

In light of above, normalization is the routinization of politics in everyday routines. Normalization could be related to the Foucauldian governmentality ideas regarding the forms to deploy and use dispositives to regulate people. These dispositives aim the equilibrium, discipline, and welfare of the population because governmentality operates through intervention to manage individuals. In doing so, it produces a biological subject, a subject whose life must be protected but also governed. Meanwhile, exceptionality could be represented by the Schmittian sovereignty ability to decree who is friend and enemy. Sovereignty can execute the elimination of people by proscription and by limiting the sociopolitical order in terms of its range and internal/external logic to define a specific enemy. Sovereignty, thus, operates by the command to secure a territory and in doing so it produces a subject of right.

Either by establishing a biological subject or a subject of right, the problem of sovereignty is still not resolved because now it hinges on the question of legitimacy, on who decides about the dispositives for governmentality or who

decides the exceptionality forms to choose an enemy. This question is extremely central to security and surveillance issues. Constructing institutions for coercion and the management of public safety are not saved from the critique of legitimate violence. Deciding on official secrets based on national security grounds is another example that raises the question of legitimacy. In that sense, Walter Benjamin interrogates the distinction between legitimate and illegitimate violence; between legally sanctioned violence and violence condemned by law. In *Critique of Violence* (Zur Kritik der Gewalt) the German word *Gewalt* refers to the English word violence but also to "the dominance, […] the authorizing or authorized authority: the force of law" (Burles, 2016, p. 139). Confronted with the question of legitimacy, Walter Benjamin and Carl Schmitt reach a similar conclusion in which authority founds its legitimacy by an initial act of violence repeated afterward. Every law is conditioned by an imposed historical origin which determines its legality and procedures. For example, the American Constitution still refers to the revolution of Thirteen Colonies against the British Empire in the XVIII century. Some continental European Constitutions are inspired in the liberal revolutions against Absolutist monarchs two centuries ago. Hence, to be considered legal, the law always must refer to the origin in a permanent circular movement. Even normalized institutions, such as the police, have their rules inspired in certain historical foundations as they should enforce the sociopolitical order continuously. Indeed, the police are a crucial example to analyze the execution of power and its legitimacy. In other words:

> In the institution of the police, writes Benjamin, founding and preservation become mixed: in this authority the separation of law-making and law-preserving violence is suspended. This is because the police are never able to simply apply the generality of the law to the specificity of a particular case. In deciding on situations that do not fall completely under the legal code, the police participate not only in preservation, but also in founding. Police violence is lawmaking, for its characteristic function is not the promulgation of laws but the assertion of legal claims for any decree, and law preserving, because it is at the disposal of these ends. In this sense, the lawmaking function of the police is exceptional, as it occurs in a situation where no direct application of the law is possible. It is this ability to decide in the face of the impossibility of the exact application of the law that constitutes sovereignty. The police, for example, intervene 'for security reasons' in countless situations in which no clear legal situation exists. As Derrida describes it, the police arrogate the law each time the law is indeterminate enough to open a possibility for them. The police thus contain, for Benjamin, the exceptional violence of foundation as well as the preserving violence of law-enforcement (Burles, 2016, p. 57).

As shown above, police institutions need to replicate the law in several circumstances that are different from each other. It means that law-creation and

law-preservation are intertwined in such a way that the borderline that separates them is blurred. Moreover, this borderline is simply abolished as the police interpretation of the law is simultaneously law-making and law-interpretation. Police action is a generative deployment of the rule but also a generating dispositive that preserves or refers to the same rule. For security reasons, security institutions such as the police replenish the governmentality and the exceptionality in politics, especially because the law does not encompasses all the situations where security institutions act and because it is impossible to assimilate and implement one single law with one hundred percent of completeness. Therefore, as expressed by Maynard Burles, there is no more pure foundation or pure position of law. In Derridian terms: "Positing is already iterability, a call for self-preserving repetition. Preservation in its turn refounds, so that it can preserve what it claims to found. Thus, there can be no rigorous opposition between positing and preserving" (idem, p. 58).

In the same way, the strict borderline between foundation and maintenance disappears. For instance, the line between Coup d'État and Raison d'État disappears because breaking with the legal order implies in deploying governmentality. Disruption is an agency of preservation by foundation. Governmentality grounded on raison d'État is not only conservation, but it also consists of "the continuous act of creating [...]" (ibidem, p. 166). The preservation carried out by raison d'État, in this sense, is done through continual re-foundations, by the regular re-creation of its conditions and possibilities. Transposing this logic to an institution like the police, it is possible to recognize that the police have a characteristic of permanent coup d'État, the defense of one exceptional moment of foundation. At the same time, the police cannot be interpreted outside the governmental rationality of preservation embodied by the raison d'État. When foundation moments lose their legitimacy and effect to preserve the sociopolitical order, thus, the police are the first institutions that strive to restore the previous foundational moment and the last one that realizes the beginning of a new era.

Considering again the law interpretation made by the police, one can express that even in the tiny administrative procedures this institution readapts the sovereign decision to the minimum details. Every judicial and administrative decision has a gray zone, a moment of indifference from the pre-established legal content. The leeway for interpretation embodied in every decision allows a strategic adaptation of the sovereignty rather than converting every decision-maker in an absolute sovereign. Moreover, the separation between the rule and its application remains not traceable in the last detail because of that leeway. In other words, the same decision encompasses normality or governmentality. At every moment, the same legal or administrative task appears repeatedly in some institutions. In that sense, exceptionality is not allocated only to especial circumstances or emergency times, neither is governmentality to quotidian

practices. As the decision on the state of exception is a political decision, which must be thought on how to apply it to a specific situation, this is equally the case for every decision and rule which tries to implement the exception in every circumstance. Thus, at the microscopic level, the relationship between exceptionality and governmentality, or the separation between them, is impossible to be established because when the exception is taken seriously, the concept lends itself to an analysis of the "infinitesimal mechanisms" of decision. In the tiniest scale of power, people are conservators and editors of rules and governmentality dispositives. Social and political life constantly escapes pre-established rules. This allows the concept of the exception to access everyday practices, to be routine.

The impossibility to strictly delimit where exceptionality ends and normality begins is exemplified in the decision taken by middle-ranked workers and public officials. That impossible distinction can be observed from the design of algorithms that process personal data, to the bureaucrat that audits companies according to the interpretation of the Law, to the police officer who decides the people that must be granted with political asylum or refugee status. That borderless characteristic can be observed in cases such as the migration police officer deciding who passes the airport controls, a human resources employer selecting new employees. Even the desolated waters of the Mediterranean Sea turn into zones of exceptionality and normality. The exceptional force of sovereignty therefore must not be interpreted at the edge of special moments. It is constantly executed at the tiniest capillarity zones of decision-making and in the plenty of landscapes of political action. The circumscription of exceptionality to special moments and places is not easy, because

> […] one characteristic that the theoretical attempts to refigure the governmentality/exception dichotomy share are that they tend to work by locating sovereignty in a particular place or time. The most well-known examples, Giorgio Agamben's invocation of the 'camp' and Judith Butler's analysis of the 'war prison,' are representative of the now-common rhetorical and analytical strategy of designating a particular spatiotemporal location where sovereignty reveals its true nature. Yet these attempts to locate sovereignty inevitably fall prey to the very spatiotemporal distinctions (norm/exception, inside/outside) they seek to escape. Claiming that somewhere or other (border, war prison, camp, reservation, etc.) is an 'exceptional space' or that someone or other (refugee, sex worker, migrant, detainee, etc.) exists in a 'state of exception' assumes too easily that a simple distinction can be made between exceptional and normal (Burles, 2016, p. 87).

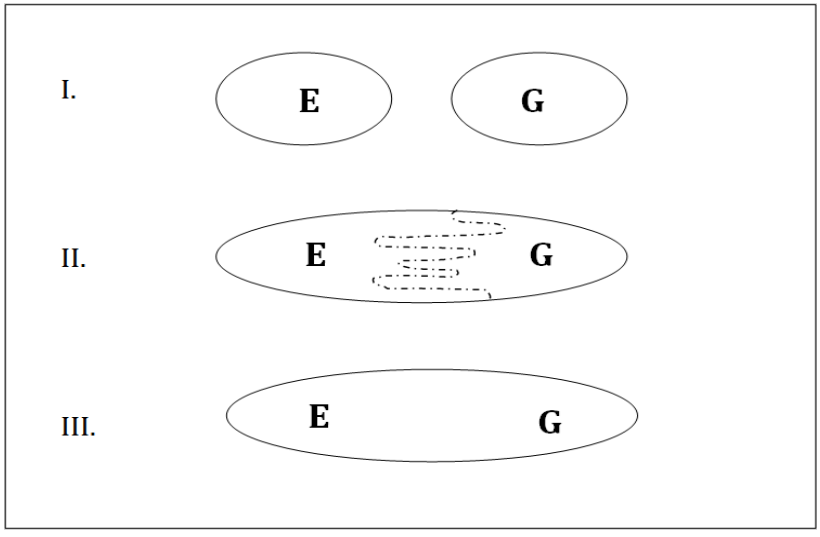
Due to the impossibility to set the borderline between exceptionality and governmentality, as they constitute every political practice, it can be said that when examined together, trying to allocate them to a certain time and space implies in an aporetic exercise: the act of demonstrating the nearly

indemonstrable. Given their relation to law, authority, and government, exploring the relationship between exception and governmentality is particularly useful for showing what and where politics is. We agree with Regan Burles in the impossibility of identifying this borderline, especially in spatiotemporal dimensions, such as special/normal circumstances and outside/inside places in the political order.

However, it does not imply that the differentiation between both concepts has been erased. The deconstruction of their particular location in the social reality does not mean that they have melted into a single phenomenon in which is impossible to recognize one from another. It is simply not possible to know where or how is the line separating them. The aporetic relation of exception and governmentality, and the problem of sovereignty, then, should not be treated as a problem to be solved, but rather understood as a flexible relationship that has existed from the first complex societies from the past to the present. What has changed is our perception and realization of the aporetic characteristic of exceptionality and governmentality.

In the same way, as classic physics interpreted certain natural objects such as the light in terms of separable properties, modern physics and quantum mechanics understand the light as a simultaneous particle-wave phenomenon. Particles and waves can be identified as separated attributes of light. Yet, they cannot be exactly differentiated at the same moment insofar as the acknowledged Heisenberg or uncertainty principle only allows the identification of one of these characteristics in a specific time. In a political allegory, the relationship between exceptionality and governmentality has changed from a traditional view to the deconstruction of its dichotomy as expressed in *Figure 1*.

Figure 1: Exceptionality and governmentality



Source: Author

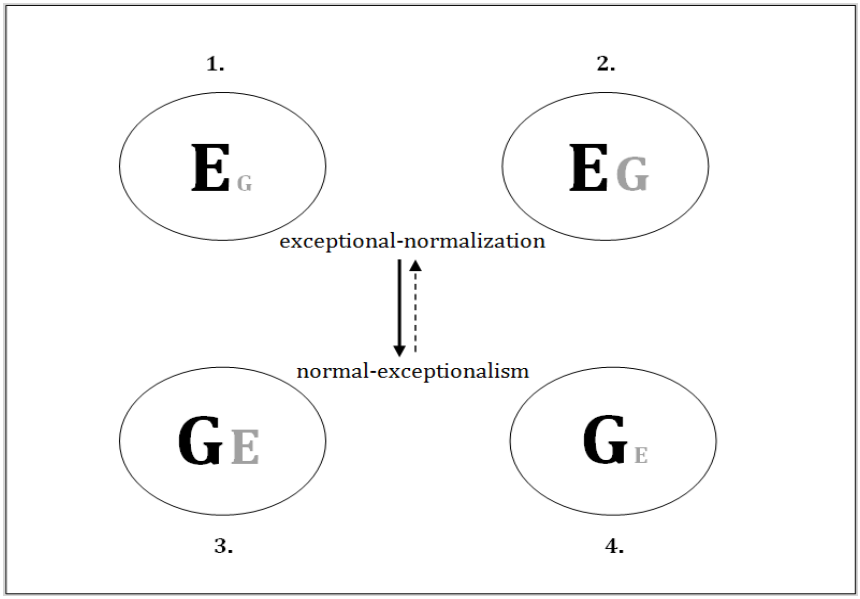
Figure 1 suggests that, traditionally, Schmittian exceptionality, "E", and Foucauldian governmentality or normalization, "G", were understood as separate attributes as in the situation *I*. In this situation, exceptionality and governmentality have a binary relationship delimited by a borderline separating singularity/normality, external/internal, foundation/routinization, coup d'état/raison d'état and so on. In situation *II*, through a deconstruction of their location and practices, and by appealing to scholars such as Wayne Burles, it was observed that exceptionality extends its dominion and melts into governmentality. In this encounter, the borderline that separates them is blurred like a surrealist image in which exceptional politics are disfigured to normal practices and normality converges with exceptionality. This blurred line is attested in the work of different scholars, as in the case in which the sovereign could decide upon the bare life (Agamben, 1998) and where the zones of indistinction between security, terror, and discipline (Diken & Carsten, 2002) spread across the planet. In situation *III*, appealing again to Wayne Burles' work, it is possible to suggest that the borderline between exceptionality and governmentality disappears because it is impossible to identify its location. Like the particle-wave dual characteristic of light, the microscopic analysis of jurisdiction interpretation and administrative decisions carried on by institutions and individuals –such as the police, the migration controller, the employer, and the bureaucrat- show that exceptionality and governmentality are a dual characteristic of politics that cannot be separated. Currently, it is considered that the wave-particle duality is a concept of quantum mechanics according to which there are no fundamental differences between particles and waves: particles can behave like waves and vice versa. In the same allegory, exceptionality-normality duality is the core of old and modern politics. There is no fundamental separation between exceptionality and governmentality insomuch the former can work and is performed through governmentality and vice-versa.

The impossibility to build a dam between exceptionality and governmentality, either by legal measures or informal practices, has a tremendous effect on the accountability effort that will be worked in this text. The aporia, the no-way or no-solution, that exists between exceptionality and governmentality points out the impossibility to deploy or think about the best practices to draw the limits of one upon the other. Creating closed compartments in the social life where governmentality will become isolated from exceptionality measures executed by disgusting or abject politics ultimately will be a naive illusion. But the fact that both cannot be separated does not mean the victory of an irreconcilable indistinctness between them. That is, even if they are not separable, the incidence of one of their poles will prevail upon the counter-part, implying situations or political practices where exceptionality proliferates at a higher level than normality (exceptional-normalization) or where the opposite occurs (normal-exceptionality).

In quantum mechanics, the uncertainty principle infers that there is a fundamental limit to the precision with which certain pairs of physical properties of a particle, known as complementary variables, such as position *x* and momentum, can be known. For instance, if the light behaves at the same time as particle and wave, there is a limit to measure both behaviors at the same instant and with a satisfactory level of accuracy. In the political world, and some physicists might agree, things could reach a degree of greater complexity. Whereas exceptionality and governmentality are intertwined, as mentioned before, it is still possible to infer the existence of exceptional and normal poles. But to what extent one can infer that a certain action or political decision is exceptional in its normality or that this same action is normal in its exceptionality? Seeking an accurate quantitative measurement of those terms in the style of physics must not be a concern of political scientists by the fact that the apprehension of the social reality works with different approaches and tools than those of natural sciences. However, it is important to avoid the indeterminism where exceptionality and governmentality are barely recognized and mistaken. The disappearance of the borderline between those features must not imply in their inconsequent confusion.

If the lack of measurement or uncertainty principle prevails to analyze exceptionality and governmentality, then we may return to the situation *II*, where it is possible to recognize exceptionality and normality but with inaccuracy or a false impression of their spatiotemporal separation (the camp, the stateless, the refugee, the postmodern world, the world after 9/11, and so on). As expressed in the situation *III*, we support the abolishment of the borderline between exceptionality and governmentality as well as their confinement to a certain place (geographic or virtual) and time (historical or invented). Both terms are simultaneously present at the same time and place in every political decision and juridical interpretation, from the top of the administration to the last hierarchy of one organization. However, this does not mean that a "top" political decision has the same magnitude of exceptionalism compared to decisions adopted in lower ranks. Thus, we postulate a variance of both terms in a typology where exceptionality and governmentality present distinct "concentrations". See *Figure 2*.

Figure 2: Samples of exceptionality and governmentality



Source: Author.

In *Figure 2*, we use the allegory of chemical concentration in the sense of liquid solutions composed by a solvent and solute. Considering that exceptionalism and governmentality are mixed and "liquid" concepts to understand the problem of sovereignty, which in turn would affect the exercise and the accountability of one authority, then they can be differentiated in a scale of concentrations.

In sample 1, the scale (magnitude, presence, incidence, or perception) of the solvent exceptionality "E" is higher than the solute normality or governmentality "G". The latter increases its concentration in sample 2 but exceptionality still prevails over governmentality. Both samples 1 and 2 are examples of **exceptional-normalization**. They indicate one action or a series of decisions in which governmentality hinges on exceptionality with the preeminence of the latter but without a clear borderline between them. Governmentality here is constructed and altered according to exceptionality. For example, the Agambian bare life, the Guantanamo prison, the martial law, and other spatiotemporal cases where exceptionality was traditionally located, continue to be exceptional ones in our interpretation. However, they also contain governmentality components normalizing the higher impetus of exceptionality. Even the illegal camps of detention have managerial tools of administration that sustain their governmentality. In the same way, the light uses the particle-wave double characteristic to reach the unobservable darkness in the cosmos and to refract across tiny folds of observable matter; exceptional-normalization can be observed at macro and micro political levels. The sample 1 is especially a sensitive spatiotemporal case in which exceptionality measures overpasses normalization. This can be observed in macro examples, such as in the Guantanamo prisons where legal procedures of a superpower were unilaterally taken inside a gray area

of the international jurisdiction, or in micro examples when police officials or private contractors act with total discretion and impunity after deviations of conduct and abuses against civilians. Sample 2 could also be related to sensitive spatiotemporal cases but on a lesser scale than in the previous sample. In those cases, the leeway to exceptional actions would be reduced if compared to the previous examples.

In sample 3, the scale (magnitude, presence, incidence or perception) of the solvent normality or governmentality, "G", is higher than the solute exceptionality, "E". The difference between them increases in sample 4. Samples 3 and 4 are examples of **normal-exceptionalism**. Both refer to actions or decisions where exceptionalism is oriented to generating politics according to governmentality premises and without a clear separation between them. That is, governmentality here conducts exceptionalism. For example, the quoted analysis of the police institution by Walter Benjamin is a case where the everyday jurisdiction interpretation must handle exceptionalism to normalize or create governmentality. Here, the exceptionalism is restrained by an impetus to manage and administrate populations by tolerated continuous exceptions. Sample 4 is a spatiotemporal case where the level of discretional and exceptional power to interpret, reproduce and redefine governmentality dispositives (such as law, administrative rule, moral value, deontological code, and so on) is very low. Sample 3 repeats this logic but with a higher leeway for exceptionality inside the governmentality dispositive. It could be said that both samples 3 and 4 –especially the latter- tend to stabilization and routinization in social systems. Yet, their interpretation should not be mistaken with rigid bureaucratic and inflexible rules that jeopardize flexibility and innovation.

In short, samples 1 and 2 seek to enhance normalization through a greater amount of exceptionality. Meanwhile, samples 3 and 4 promote normality with a lesser amount of exceptionality. These samples try to solve the postmodern problem of indistinctness between normalization and exceptionality. They introduce degrees where traditional dichotomies are replaced by "liquid" solutions as components of political decisions. These ingredients are so intertwined that they are not separable even by a blurred line. Moreover, from our perspective, normalization dominating exceptionality could be deemed as the goal or the horizon of politics, even if this scenario is not temporally permanent or fully accomplished (see arrows in Figure 2).

The more politics promotes *exceptional* measures, the more it aims to reach *normal* politics (full downward arrow). That is, exceptional politics also has the intention to create or restore a scenario of *normal exceptionalism*. Even disgusting and violent politics pursue ulterior goals or "good" objectives. If political revolutions (like those committed by groups of the different political spectrum in the last century), and the creation of exceptional powers in one organization (like

intrusive surveillance and unchecked powers of security agencies), enhanced violent politics in history; it is because these exceptional examples intended to normalize an ulterior panorama (either for the sake of social justice, liberty, welfare, or security). Rather than absolving their intentions and their actions, it just indicates that normalization is pursued even by greater amounts of exceptionality. However, since exceptionality cannot be separated from governmentality, and vice-versa, those attempts withhold societies or sent them back to the exceptional-normalization category of disgusting politics (dotted upward arrow). In those circumstances, governmentality was executed through greater concentrations of exceptionality, including the use of abject methods like the adoption of vicious circles of violence.

Let us address briefly another concrete example: the management of refugees in recent years in the European Union. According to authors such as Giorgio Agamben (1998), refugees are figures that embody the exceptional forms of power as they relate to his conception of "bare life." For Agamben, the refugee is removed from the political realm and exists in opposition to those persons within a particular mode of life or qualified life. The refugee is the biopolitics figure who is deprived of social, political, and economic rights. Oppose to Agamben, Seth Holmes and Heide Castañeda argue that refugees are multiple and diverse, and they are differentially involved in making political and symbolic claims. For those authors, refugees are not simply exceptional "bare life" removed from the realm of the political, but "political actors whose subjectivities are shaped by the uneven social and symbolic environments in which they simultaneously are positioned and position themselves" (Holmes & Castañeda, 2016, p. 20). In addition, for Carl Levy, the refugee policies in the European Union are not as straightforward or as stark as in the interpretation of Giorgio Agamben followers" (Levy C. , 2010, p. 97). According to Levy, the regression of the liberal state to a universe of camps in the Eurozone is not happening as this interpretation failed to capture the entire social reality.

In our vision, Levy understands Agamben´s state of exception only in terms of bare life. However, sovereign powers do not act only by excluding and turning subjects into bare life. Bare life is only the tip of the iceberg of a sovereignty that works across several domains deploying visible and invisible governmentality tools to administer "outsiders" and "exceptional" individuals. Indeed, the refugee's situation was not shaped only by extraterritorial zones and states of exception. The borderlines of the EU are porous and many of those subjects were politically assimilated regardless of controversial points such as cultural integration and security concerns. However, if refugees are as diverse as other groups, this diversity does not entail in a heterogeneous treatment in the face of official powers. Comparing to other groups, official rulers speak of the refugees homogeneously, implementing heuristic tools and legal norms that are guided by discourse based on suspicion. The refugees are a collectivity that coalesces the

management of the “different”, the “new”, the “strange”. In that sense, a Euro-Mediterranean system of management was created to handle those subjects. Lives perishing in the Atlantic, the Mediterranean, and the Sahara are just one sinister form of administration compared to the chain of extraterritorial camps and legal agreements that were established with third countries, such as the one signed with Turkey in 2016 to restrain new waves of refugees from the Middle East. In that sense, exceptional bare life is just one piece of a puzzle where sovereignty is capable of deploy exceptional but also governmentality measures to manage refugees. For example, joint naval patrols or bilateral agreements are tools oriented to groups that are treated in a specific form when compared to tourists and economic migrants. Integrated Border Technologies, formal rules to distribute refugees within State Members (Dublin Pacts I and II), informal detentions in camps, and even illegal human smuggling are visible and invisible governmentality tools that work for the sake of exceptionalism. In short, if refugees cannot be considered as simple subjects of exceptionalism, they awake exceptionalism responses even by governmentality trends. In conclusion, their treatment would correspond to samples 1 and 2 in the figure above. To manage these individuals, exceptionalism promoted by governmentality tools seems to be accurate to define their situation even if one can detect a multi-level series of statuses to handle this group. Rather than being at the fringes of the society to come, refugees might embody the re-foundation of the European Union at the core of its sovereignty.

The samples in the figure must be understood in symbolic terms. However, the terminology used in the figure could be used to assess the management of subjects, as in the example related to the refugees, or in domains that traditionally were considered either as normal or exceptional ones. Therefore, rather than a exceptionality-governmentality dualism, the categories of exceptional-normalization and normal-exceptionalism can be useful to shed light upon the microscopic and macroscopic aspects of politics. For example, this work will explain why the most common dispositives of governmentality to manage personal data of “normal” citizens are permeable to exceptionalism. Categorizing and sorting “normal” individuals is not detached from generative moments of foundation and re-creation of macro-politics. At the same time, this work will show that the most exceptional measures to manage “exceptional” people by security and intelligence services are composed of governmentality trends that “normalize” their situation and redefine the political order as a whole.

From the discussion above, it is possible to draw two important claims:

1) Exceptionalism can be expanded through governmentality and vice-versa because they constitute an inseparable dual political phenomenon.

2) Normalization seems to give an orientation to this dual phenomenon, even when exceptionality overcomes governmentality through abject methods.

One can argue that those claims still do not answer correctly this: how does one differentiate exceptional normalization and normal exceptionalism? This work insists on maintaining the identification of exceptionalism and governmentality despite the abolishment of the borderline between them. In our interpretation, both terms are present at the same time and location of a political decision, yet they have different concentrations. The samples above are symbolic representations of those concentrations and serve as an allegory of elementary particles contained at the very nature of micro and macro politics.

Under a microscopic examination, rather than solving the aporia of power, we have shown how to understand its duality. Thus, one must be skeptical about decisions that seem normal. Each governmentality action promotes exceptionality by distinct concentrations. Even the best intentions and banal attempts to improve our political world are not disconnected from exceptional re-creations. Thus, the main idea now is to recognize that one political decision is at the same time exceptional and normal, instead of purely delimited to one of those terms. This idea entails two big consequences.

Firstly, the dual characteristic of power means that utilitarian approaches in politics fail in one important fundament: the clear separation between means and goals. Political decisions that seek for ulterior goals, separating or ignoring specific methods and means, imply in separating the impossible. For example, “good” ends do not excuse “bad” means because these steps deploy, at the same time, governmentality and exceptionalism that redirect the evolution of politics to unforeseen consequences. In that case, it is even possible to reach huge levels of exceptionalism just by promoting controversial and normal decisions every day. The exceptional normalization category can be reached by incremental steps. Policy-makers, security officials, and practitioners should take into account this consequence.

Secondly and lastly, if one wants to control or tame completely a certain power, it will be an attempt to control the uncontrollable (again). Power has a dual characteristic (governmentality-exceptionality) that cannot be separated or circumscribed with precision. The lack of that separation implies that sovereignty (not only of states and nations) can be performed by expected normal exceptionalism and also by unexpected exceptional normalization that escapes from the best rational practices, rhetorical arguments, and institutional designs. Decisions can be restrained, redirected, and replenished, but they cannot be controlled in their integrity and in their sequential repetition (routinization of decisions). Human beings are, at the same time, enhancers and editors of decisions. For good and evil, power, as light, runs across the “infinite” darkness of the universe but also overcomes the “microscopic” barriers built against it. Thus, rather than solving the aporias of power, accountability must assume its limited characteristic as a restraining tool. Accountability, thus, is an instrument to

redirect and give orientation to power instead of a corrector. Even when controlling the uncontrollable seems impossible, restraining mechanisms such as accountability have the potential to redirect the concentrations of exceptionality and governmentality.

In this section, we have shown how exceptionality and governmentality converge to execute power. Yet, we still need to address the question regarding the legitimacy of power. In other words, how a sovereign justifies the execution of power? This issue is closely related to accountability, the action of restraining and redirecting power. Thus, to answer this, we need to depict a brief history related to the justifications and forms to legitimize power.

1.1.c. Justifying power: A brief epistemological history

What sustains the power of sovereign entities that command people? Force, coercion, lies, fear, tradition, respect, tolerance, all those words might explain partially the characteristics of power but they do not address its foundational direction. To answer that question, one component that moves power is the gap between its actualization and promise. That is, a sovereign power have many characteristics, yet, it also justifies its existence according to the principles that orient its action and development. Without a normative component, a promise, the sustainment of power would be empty. Without the desired way to transform things, exceptional and governmentality tools would lose content and function. In this section, thus, we make a brief history of the main normative components that justified the execution of sovereignty. This chronological section is crucial to understand the evolution of the contemporary forms that sustain authority, the object of accountability.

The belief in the supernatural was present in the first human groups. But the idea of an omniscient entity who guards morality is more recent. Before the Neolithic revolution and the emergence of agriculture, humans lived in relatively small groups based on kinship. In the "tribes", everyone knew each other and it was difficult to have antisocial behavior without being caught. The risk of being identified, punished, or expelled from the group was enough to control someone. There are some groups, like uncontacted tribes in the Amazon, who still might live in this way. But the vast part of humankind trailed a path in which relations with strangers grew and, at the same time, the chances of escaping sanctions. For many scholars of religions, the appearance of a divine entity who sees everything worked as a social amalgam, a glue that facilitated the emergence of complex and larger societies, either to discipline people (Purzycki, Apicella, & Atkinson, 2016) or to spread virtues and morals (Lyon, 2014). That is, surveillance of people by an external and supernatural entity was one of the most important milestones in anthropological and moral terms. From early times, living in society implied in

surveilling and being surveilled. Surveillance, in turn, implied in domination and power relations between individuals in many contexts.

In ancient Rome, Juvenal famous quotation "who will guard the guards themselves" (*Quis custodiet ipsos custodes*) is one of the earliest seeds planted in the Western culture referring to restrain power from a specific watcher. In that verse, present in *Satires VI*, the ancient poet questions if a male can oversee his instinct to punish a woman due to the decay of feminine behavior and virtues.[2] Since then, this quotation became an allegory of watching powerful people. It became "watching the watchers", the act of staying vigilant against those who observe and control someone else actions. Later, it became a motto that reminds the importance of restraining oppression and even tyranny. Nevertheless, there is a better reference to controlling power in the same work. In *Satires XVI*, Juvenal exalts soldiers as they are located above the law and are immune to justice and to the command of family patriarchs. Unlike civilians, soldiers were shielded from civilians' accusations and embodied an authority that barely had limits.[3] Despite their visibility in regular life, Roman soldiers were barely controlled, especially by those without influence and privileges. To be accurate, since the Second century neither Juvenal nor other writers had "watching" powerful people as a main concern. If sovereignty is as ancient as the first human groups, only in the recent centuries, since the Modern era, controlling the powerful ones was transformed into a mundane object for powerless subjects.

In the Modern era, Nicolao Machiavelli opened a line dissociating politics from morals in the 16th century. In *The Prince* and *Discourses*, his major texts, Machiavelli stated that "a prince who wants to do great things needs to learn to cheat" (Machiavelli, (1532) 1996, p. 218). Hence, power overcomes morality was also based on the pragmatism of the ruler. However, he also defended the virtues and good habits as a guide for action: "As good morals to be preserved need laws, in the same way, the law needs good habits in order to be respected" (Machiavelli, (1532) 1996, p. 84). Ethics in Machiavelli is judged through the motivation of actions and through the virtues of consequences. For example, in periods when the social order is relatively stable, morality can be raised within the context of the norms shared by the community. Yet, the norms themselves are questioned and tested against their inner criteria when especial circumstances demand to do so. From Machiavelli, the guiding idea of power should be the virtues of citizens, unless exceptional and hard situations demand to change the norms. In that sense, the exceptions deployed by the ruler to alter normality by emergency measures were justified in Machiavelli's ideas.

[2] "I hear always the admonishment of my friends / Bolt her in, constrain her! / But who will guard the guardians? / The wife plans ahead and begins with them." Satire IV, Juvenal. See: Braund, 1992.
[3] Satire XVI, lines 16: 35, Juvenal.

However, the sovereign power cannot establish exceptional measures only based on particular criteria. Within the tradition of classical liberalism initiated in the Modern era, the state is functionally legitimized as it guarantees freedom and property rights. To accomplish these actions, the state needs, among other mechanisms, a police institution. Yet, this involves two problems: firstly, the sovereign state needs to pay the police through taxes that undermine the right to conserve property or salary. Secondly, it must punish disorder through fines and penalties, but this action undermines the principle of the right to liberty. Consequently, a new layer of legitimation of the sovereign state is needed as the only functional perspective of enforcing rules is not sufficient.

Additional layers of legitimacy arise from social contracts and subjection contracts (Heywood, 2016). In the former, free citizens agree on a contract from which the sovereign power emerges. In the latter, free citizens agree to establish a contract with a third entity that does not represent them directly and from which political power arises. In that sense, Thomas Hobbes has formulated perhaps the most important contract in political and philosophical terms. The Hobbesian contract is a mixture of the two mentioned types of contracts. In this agreement, there is a transfer of partial rights to the Leviathan, the governing entity. The Leviathan can be understood as an indirect mechanism of individual rationality mediated by a third entity, it lays the philosophical foundations to justify a sovereign state. In this contract, the right and the reason for the "state" rise directly from blocking the realization of the individual meta-preferences in the "state of nature", the violence of individuals against each other. Men holding back their impulses and wishes in favor of a regulatory entity is the first mechanism of massive self-control in the Modern era. The Leviathan means giving up certain power methods over other ones in order to attenuate violence and promote what the state of nature really seeks for: peace. This implies that the state can only ensure peace only if it is the owner of the right to everything. In this task, Hobbes implicitly affirms that a true sovereign needs to secure the monopoly of violence. Violence and ruling are central as they could be executed without constraints if a sovereign is to accomplish the social contract.

> [...], that king whose power is limited is not superior to him, or them, that have the power to limit it; and he that is not superior is not supreme; that is to say, not sovereign. The sovereignty therefore was always in that assembly which had the right to limit him, and by consequence the government not monarchy, but either democracy or aristocracy; as of old time in Sparta, where the kings had a privilege to lead their armies, but the sovereignty was in the Ephori (Hobbes, Leviathan (Longman Library of Primary Sources in Philosophy)., (1651) 2016, p. 119).

Sovereignty, then cannot be summarized to the ruler's willingness. More than being connected to rules, sovereignty stems from a relationship of power

between ruler and subjects (or government and governed, or watcher and watched). As Hobbes writes:

> From this institution of a Commonwealth are derived all the rights and faculties of him, or them, on whom the sovereign power is conferred by the consent of the people assembled […] Because the right of bearing the person of them all is given to him they make sovereign, by covenant only of one to another, and not of him to any of them, there can happen no breach of covenant on the part of the sovereign; and consequently none of his subjects, by any pretence of forfeiture, can be freed from his subjection. (Hobbes, Leviathan (Longman Library of Primary Sources in Philosophy)., (1651) 2016, pp. 107-108).

Hobbes, therefore, opens the Pandora box transferring the sovereignty power from dispersed political elites and groups to a more unified branch specialized in incorporating the role and the execution of the social contract. Since then, this specialization has been refined until nowadays. In Hobbes, the subjects need to transfer rights to the Leviathan in order to avoid mutual and unrestricted violence among them. In the Leviathan, justice is equivalent to legality but cannot be reduced to it. One illegal action or illegality means breaking the contract with the sovereign as attested in the last quotation. Legality is understood as a consequence of the subjugation of individuals towards the Leviathan's willingness and sovereignty. And this sovereignty legitimates itself insofar as it avoids the worse facets of the state of nature. In Hobbes, the idea that the social contract needs a priori virtuous citizens, as the heroic moral virtue of philosophical rulers in the Antiquity or a religious faithful king as in the medieval era, is abolished following the splitting line opened by Machiavelli between moral and politics. In that split, to politics, the virtuosity of those who govern or are governed became a secondary point. Thus, it was essential to create a social contract considering the worst moral situation of individuals in order to construct a public order. And this is not because men are morally corrupted by nature but because the political order should consider all the circumstances to govern, including the worst-case scenarios of morality.

Going forward in time, during the independence of the United States of America in the 18th century, the authors of the *Federalist Papers* (Hamilton, Madison, & Jay, 2008), in their comments to the constitution of the federal government, reacted to the previous moral question in a straight answer: when virtue does not have roots in citizens, it needs a substitute. For them, the lack of virtue of citizens could be replaced by an arrangement of institutions in which the passions and egoism that undermine freedom and property are checked and reciprocally counterbalanced. It is the birth of the system of checks and balances between government powers that have been inherited to us today. That system – inherited in turn from Enlightenment thinkers like John Locke- take down the common assumption that political theory is not connected with practice or that it

only leads with abstract ideas. John Locke, for example, worried by the clashes between the Monarchy and the Parliament in England during the 17th century, advocated the separation of functions between the executive and the legislative tasks of the government. In a time of internal wars and turmoil, the fact that the Crown budget and important laws started to be approved by a legislative institution was a model inspired in his theoretical efforts. For Locke, the legitimacy of power stems from the willingness of freemen subjected to the rule of authority. Moreover, in *A Letter Considering Toleration*, he puts the focus on restraining sovereignty power when it comes to religious practices and the coexistence of different faiths between authority and subjects. Sovereignty, according to Locke, has limits and must be rightfully conducted (Locke, (1689) 2012).

Another example from the Enlightenment era comes from Immanuel Kant. In Kant, the social contract is not based on rational and utilitarian grounds but in moral imperatives that enhance individual freedom. This freedom is attached to following mandatory rules in favor of moral precepts. A person who did not abide by any rule and only followed basic instincts was slave of them (Kant, (1781) 1998). For Kant, the social contract and the rules are valid by a deontological orientation to guarantee individual freedom, the right to gain and live under a state, and the moral duty to preserve the liberty of other individuals in society. Liberty, thus, is circumscribed to a sociopolitical order and present limits (Kersting, 1992). Kant recognized that individuals' liberty is a priori condition for all human beings, understanding that "each individual is equal to other ones in the condition of its citizenship, thus, the citizen must have his autonomy respected" (Kant, (1781) 1998, p. 224). Those moral imperatives are one of the maximum expressions of beautiful politics that were formulated in a time when they barely could have been recognized and applied. They indicate a development that was to be incorporated in future norms and constitutions of countries. Unlike men, ideas can be "immortal".

The separation of powers in order to build a social contract was also deemed as a form to avoid tyranny. However, the evolution of this system was reduced during the Cold War era and it is still being improved in our times. The competition between Western and Eastern political systems during the last century was mainly a confrontation between liberal democracy and real socialism. In this clash, inner institutional designs, such as the checks and balances system, were put in a second level whereas legitimating a sociopolitical order encountered a raison d'état in the confrontation against external foes and economic ideologies. The competition between external systems, therefore, implied the need of external legitimacy or the "verification" that the rival system either curtailed individual freedom or social rights. Legitimacy, during the Cold War era, was mainly based on the "comparison" with the external adversary.

In this perspective, after 1989, the collapse of real socialism in Eastern Europe produced two consequences. First, this collapse increased the need for Western democracies to justify their internal normative foundations and their liberal systems. With these normative criteria, the deficit and the 'pathologies' of western democracies, as the separation of powers and the social inequality, returned as focus of concernment. Secondly, and more importantly, this collapse allowed verifying that there is not a single model of liberal democracy (Klingemann & Fuchs, 1998). Although this model has been promoted since the liberal revolutions of the 18th and 19th centuries, questioning the quality of this type of democracy has emerged only in the late 20th century as an important political trend.

However, even before the collapse of real socialism, some scholars of liberal democracy were already concerned not only in the dysfunctions of this kind of democracy but also in its foundations. In liberalism, for example, freedom has an essential function as the ultimate foundation of all political society. But what is the core of freedom or what kind of freedom is necessary for this system? According to Isaiah Berlin, one central aspect of freedom is denominated "negative freedom". Negative freedom is owned by individuals insofar as they are free from external interference. Apart from natural, social, and political external interferences, when it comes to sovereignty, negative freedom indicates the existence of resistance rights that the individual owns against the state. These rights are zones in which the state cannot intervene and must protect and guarantee its inviolability (Berlin, 2017). In addition, negative freedom implies freedom of choice. Freedom of choosing between two options is certainly less important than choosing between one hundred alternatives. Consequently, negative freedom also means holding the burden of choice. Negative freedom is important in the sense to establish a legitimate action of response and even disobedience against traditional sovereign forms such as the state. The exercise of this action has been present in many historical events of contestation.

Another essential point in the encounter between sovereignty and subjects hinges on the idea of intrinsic equality. This idea questions to what extent there is a priori sense of equality stemmed, for instance, from Kantian moral imperatives such as citizenship based on equality. In that line, for Robert Dahl, the best democracies were those who altered to a lesser scale the principle of intrinsic equality. In *Democracy and its Critics*, he proposed several criteria and institutions to respect the equality principle. In his view, democratic institutions should specify the establishment of elected officials, free and fair elections, inclusive and passive suffrage, freedom of expression, alternative information, and free association (Dahl, 1989). During the nineteenth and the twentieth century, those criteria were gradually recognized as democratic procedures and were assimilated in the Constitutions of hundreds of countries. But this was only achieved after struggles and severe clashes, like the ones promoted by the Suffragette movement to obtain

the right for women's vote in political elections. Dahl´s democracy, in short, is a path to implement and improve the mentioned criteria and institutions. At this point, sovereignty is disarranged according to the equilibrium of distinct forces and by several political procedures. However, a democratic scenario that accomplishes only these criteria could be a poor one, especially if we attach sovereignty and democracy to procedural and institutional precepts. Democracies should strive for substantive values to nourish their procedures and institutions. In that sense, and admitting that the next statement does not make justice to Dahl´s work, even totalitarian regimes can fulfill democratic procedures with a considerable range of acceptance.

Totalitarian experiences are the paradigmatic example of exceptional politics produced by unaccountable sovereignties in the last century. In *The Origins of Totalitarianism*, Hannah Arendt analyzed fascism and communism as variants of the same phenomenon. This parallelism is debatable; nevertheless, it presents relevant points. In totalitarianism, sovereignty does not try to get subjects but to eliminate them as individuals (Arendt, (1951) 1973). Arendt was concerned with the elimination of freedom as an authentic element where human beings can live among equals. Totalitarianism did not change the concepts of crime, guilty, and innocence as dictatorships and despot rulers did. Those criteria were simply eliminated and substituted by concepts such as "unwanted" or "unworthy live", whose disgusting consequences, as we mentioned in the first section, cannot really be represented and internalized. Moreover, totalitarianism was not simply a vertical system of organized violence. Violence here was driven by the implementations of new procedures –such as political police, and a network of espionage linked to the major party- upon previous institutional structures in order to create a permanent state of exception (Agamben, 1998). In our perspective, totalitarianism was not only the continuation of exceptional measures. It proposed new normality, new governmentality to administrate populations with higher and disgusting concentrations of exceptionality.

Considering the effects of totalitarianism, Arendt and other theorists focused their attention on the performance of individuals as persons of virtues who live in society. The separation between morality and politics was no longer admitted but it was far from being resolved. Meanwhile, the liberal stream specialized in designing institutional models to control the imperative of sovereignty and improve a certain type of democratic action. An example of the junction of these two fronts, between virtues and institutional designs comes from Benjamin Barber. In *Strong Democracy*, politics is understood as a form of participation where conflict is solved by the creation of a political community, a place capable of transforming dependent individuals into free citizens and partial interests into public goods (Barber, (1984) 2003). Active citizenry in politics, for Barber, determines the difference between a Liberal representative democracy based on elections and a strong democracy based on participation. Therefore,

Barber's efforts try to promote active citizenship and rescue civic virtues in politics.

To avoid tyranny and considering that citizens cannot be efficiently active all the time, other theorists designed a scheme of values focusing on justice. Due to the heterogeneity of societies, in *The Spheres of Justice* by Michael Walzer, social practices that consolidate a "good" life are constructed and distributed unevenly among people. These goods are built in different spheres that need to follow internal rules of distribution. Each sphere has a specific justice and moral logic of distribution such as free exchange, merit, and needs, which can determine different political practices such as market, labor, and education (Walzer, (1983) 2008). Injustice problems arise when one sphere monopolizes the rest with its internal logic, promoting inequality and dominance. For Walzer, the balance between the spheres of justice represents a complex system of equality to prevent tyranny. Walzer is a liberal communitarian who supported liberalism as the art of separation. “Liberalism is a world of walls and each of them generates new freedoms” (Walzer, (1983) 2008, p. 38). The idea of moral spheres aims to reconcile the representative democracy and the system of checks and balances with the promise of equality. If in the traditional liberal democracy human beings are deemed as subjects of isolated rights, Walzer transferred the system of checks and balances from institutions to people. He developed a theory of political community where spheres of justice avoid that one of them (i.e. money and economics) hijacks the logic of other ones, disintegrating justice among human beings.

Parallel to liberalism, critical theories have also analyzed the relationship between subjects and sovereign powers. During the first half of the twentieth century, if philosophy proposed the emancipation of human beings, it was because of Marx's and Freud's ideas. For them, humans need to free themselves from the historical immaturity and domination. They must be able to achieve an autonomous and realized life. In that sense, critical theory was simultaneously in favor and against the Enlightenment tradition. For example, Max Horkheimer and Theodor Adorno, theoreticians of the Marxist Frankfurt School, expressed that the Enlightenment did not establish the kingdom of freedom. Rather, among its consequences were two world wars and totalitarian dictatorships. Enlightenment and rationality had a dark side at the service of disgusting politics and to the objectification of the world and its people. Market and capitalist consumerism, for example, were denounced since the 1930s as a veil that obfuscated or alienated individuals in different ways (Horkheimer & Adorno, (1947) 1972). To reach this interpretation, it was not mandatory to be a radical dissident, it was only necessary to elaborate criticisms like those of Jürgen Habermas, who in the second half of the century, observed that rationality, consumerism, and alienation affected everything, including the political communication.

Initially influenced by the critical theory of the last century, Habermas developed a multi-theoretical approach to several political phenomena and moved away from critical perspectives. In *Between Facts and Norms* he questions of legitimacy and legality of the state appear as his main concernment in a time of globalization and transformation of regional and national spaces (Habermas, (1991) 2015). For him, the legitimization of Rule of Law emanated from the people but especially to legal procedures. For him, people must submit to the Rule of Law insofar as they have participated in their creation and destination. The citizen is, at the same time, the receiver and the author of state procedures. This idea that sovereignty emanates and must be conducted by the people is not new. Yet, Habermas attributes to the judicial sphere a self-legitimization characteristic and a decisive function to conduct the preferences and participation of active citizens. Hence, institutions such as Constitutional Courts are to protect the Rule of law but, at the same time, they should not be opaque before the population at the expanse of becoming technocratic machines. When a political decision is taken for everyone, everyone must speak to enhance that decision (Habermas, (1991) 2015). In this perspective, only when citizens enjoy full rights of protection and participation, then one can define this scenario as a democracy. Therefore, the condition of the rule of law cannot be reduced to mere rights of protection that allow individual autonomy. Rather, individual and public autonomy are mutually dependent and complementary.

The Habermasian democracy stream based on deliberation and participatory citizens has enriched the understanding of democracy, legitimacy, and the authorization to execute sovereignty. However, the hope that deliberation and participation receive in this democracy is shadowed by the limits of the conflictive and heterogonous public sphere and by mass culture alienation. In *Democracy and Deliberation*, James Fishkin infers that deliberative procedures enhance the moral quality and virtues of institutions and the execution of sovereignty. But he admits that the current situation of mass culture and media preferences do not correspond to the expectations of a real discursive public sphere. For Fishkin, the more a policy orientation is based just on 'immature' or prepolitical preferences of citizens, the poorer is the quality of politics. The citizens of Western democracies, to him, have become rational ignorants. Besides, politicians' approaches seek to fulfill selfish and rational preferences of voters ignoring the common welfare (Fishkin, 1991). The problems to improve deliberation and participation in democracies are found in other examples and scholars; however, size and technical limitations must not be mistaken as a substantive problem of participative democracy itself.

Liberal and critical streams have been essential to understanding some points attached to the problem of sovereign power (especially from states), as the problem of its authorization, execution, and control. To conclude this brief history, let us introduce the last stream that contributed to this matter: post-modern and

post-structuralism theory. Despite their differences, this stream was developed since the 1970s to understand power and sovereignty via hidden or invisible mechanisms. For example, rather than a monolithic entity, the execution of sovereignty has several forms beyond regular institutional dimensions. It is enhanced by rhetorical, discursive, heuristic, and genealogic tools that could be unmasked and reconstructed. One of these attempts to unveil power was made by Michel Foucault in the late 20th Century. Opposite to what is stated by official politicians and bureaucrats, for Foucault, power is not something that one can be appropriated, possessed, or inherited; it is not something that can be localized, for example, on the top functions of a political structure neither does it work through subordination. "[P]ower is never completely found in one site" (Foucault, (1984) 2019, p. 40). We have to understand power, according to Foucault, as a flexible and subterranean mechanism that can be conducted by many people. The norms (legal doctrines, medical diagnosis, and teachers' speeches) are effective because they carry a non-visible component that conducts and constitutes themselves as a means *of* power, not *for* power. Therefore, this subterranean component breaks with the Enlightenment and Marxist dream that interpreted norms and rational actions as mechanisms that can tame reality for the sake of human reason and emancipation. In Foucault, critical statements against the concentration of power in a superstructure of domination do not imply in the art of "not being governed in any way" (Foucault, (1984) 2019, p. 12), but in the substitution of the mechanisms of power without altering its very nature.

Even topics that were previously taken for granted passed through a process of deep examination as in the case of sex. When biological characteristics can no longer explain sex because it is attached to social constructions, this does not mean that the individual can freely choose sex. Images, ideas, stereotypes, and other dispositives are understood as shared imperatives or "spheres of social coercion" (Butler, (1990) 2011, p. 132). They surround the individual as a solid castle difficult to be deconstructed. The private spheres of people, thus, are attached to social and public dimensions. Normality and exceptionality categories are intertwined and cut across biological subjects. In that sense, shared ideals of love, marriage, and sexuality are as pertinent to examine sovereignty over people as geopolitical and national security matters. Sovereignty is deployed over bodies and is seen everywhere, not only on state forms. These representations are even reproduced and repeated as the use of our mother language. Likewise, sex, gender, and language, power is fragmented and repeated in tiny gestures and re-created every day.

In light of the above, when identity concepts such as "women" or less traditional ones such as "women intelligence analysts" are addressed, those matters also affect bureaucracies and traditional policies. For instance, Judith Butler infers that feminism needs to be thought with "strategic essentialism" instead of "ontological essentialism" (Butler, (1990) 2011, p. 93). That is to say,

people should act according to strategic calculations of their subjectivities *as if* their aspirations truly correspond to the essence of their identities in the real world. In that sense, people should struggle for something even if the inputs and outcomes of the struggle are not fixed. This same logic could be applied to women's and minority rights even inside institutions of surveillance and intelligence. A group needs to adapt its strategies according to other groups and circumstances. Moreover, and assuming that many security and intelligence practitioners would question the existence of this paragraph, strategic essentialism in the case of feminism is like a struggle to re-create sovereignty and the social position of women; as in the effort to avoid the concentration of power in institutions ruled primarily by men. This margin of disengagement and strategic approach has the potential to alter real practices of power between subjects, and not only for the sake of women. In this perspective, sovereignty cuts across institutions, rules, bodies, sex, and distributes normality and exceptionalism in concrete but mutable identities from people.

The non-static relationship between subjects and the characteristics that surround them is also found in the case of the deconstruction of language. According to Jacques Derrida, we must not imagine the meanings and contents of language as relationships of static constructions but as a tremulous totality (Derrida, 1978). Since the classical Greek antiquity, Western culture has sought a firm ground, the essence of the understanding of things. This understanding based primarily on reason -logocentrism- adjusts itself to power by excluding otherness, alternative evidence, and the multiplicity of interpretations. But once considered, even solid terms, such as "national security", "official secret", "public good", are transformed into amalgams of different meanings that can be questioned and deconstructed. From fixed words, we passed to polyhedric ideas of diverse edges and hidden faces (Derrida, 1978). This movement, called deconstruction, takes down different mental conceptions. Even in solid physical constructions, there are imperceptible cracks that demolish buildings over time. The understanding of language, therefore, matters to analyze politics. Even language is a reflection and a mechanism of power. In addition, the interpretation of language and its terms never finishes. In fact, in the philosophy of deconstruction, "understanding" is always aporetic, it lacks an absolute and permanent solution.

On the other hand, for Derrida, there is no separation between the foundation (creation) of justice and the procedures (repetition) of justice. To legitimize law, some entities affirm having the right to establish the norms and build a legal system. As every foundation refers and repeats itself by appealing to that origin, every legal decision is a promise (to enact and follow the creation of rules). When one of those terms, creating and repeating, is deeply questioned, the foundation of the institutional body of laws and the sociopolitical order as a whole collapse. In that light, for Derrida, the legal decisions of justice want to bring elements that remained out of its range to overcome/improve the old legal order

by creating a new “layer of law". Every upgrade of the legal order is processed within the legal order. Thus, there cannot be anything outside the law (Derrida, 2010). This explains why exceptional measures, such as in anti-terrorism, are not strange to judicial expansions and have vague terms to encompass broader phenomena (virtually everything). Nothing can escape to sovereign power, at least in potential terms. Notwithstanding, in Derrida, democracy as a promise is also a paradox. This kind of government can never be taken for granted or as fully accomplished. Democracy is not a finished order but an open promise, it is always a pending destination (Caputo, 2003) (Derrida, 2010). Democracies become violent and fake when they interpret themselves as closed and completed systems. For this reason, democratic sovereigns should always justify their power and give accounts of their actions permanently.

If sovereignty and language can be deconstructed in many interpretations, it is in Niklas Luhman where one can find its illusions. For Luhman, communications define the indivisible part of current societies. In the 70s, he wrote that we started an era where human beings are no longer the central element but communication. As communications continuously reproduce and define the scope of social systems, there is an “autopoiesis” of systems, a movement of continuous expansions, and self-reference (Luhmann, 1986). The activity of intelligence, for example, could be framed as an example of the autopoietic system since communication and analysis of objects recreate and expand this system. Intelligence produces intelligence and differentiates from other systems by the products and its replication capacity. In addition, systems can have points of confrontation and misunderstanding with other ones. Whereas systems seek to differentiate themselves from other ones, they create the conditions to increase the complexity or entropy of societies (Luhmann, 1986).

In his posthumous book, *A Sociological Theory of Law*, Luhman refers to the political system (i.e. government, intelligence) as an illusion of sovereignty. That is, the political system is just one social system among other ones. Hence, politics cannot cause real changes or command the other ones. The political system cannot effectively lead other systems because of the clashes and conflicts between them. In addition, the principle of differentiation between them prevents effective leadership apart from influences and regulatory mechanisms that guide (without defining the course) of other systems. Besides, as the political system does not know all variables from social reality, it reconstructs and survives because of a systemic and necessary illusion (Luhmann, 2013). This system affirms to the rest of society the things it can change. “Yes, we can” has to be repeated in politics even when it is *de facto* impossible for one system to change other. This illusion does not stem only from the voters themselves but also from the policy-makers and politicians that are really convinced of that dream.

To a certain extent, the fictional nature of sovereignty is clear in the role of the state, either in the strongest ones or in failed examples. Since Hobbes, the state has gained a sacred meaning, the exaltation of the idea of sovereignty that had a function of autosuggestion. That is, if a state is responsible for the welfare of the entire population, this idea opposes the principle of differentiation in a system (Luhmann, (1999) 2012). Then, as a legal construction, the state would be a mere illusion based on a Constitution. "From the functional point of view, the state is a fictitious unit, a trick of adjudication in which politics and law are used in different ways" (idem, p. 391). Luhman alert us about the illusion of a powerful and efficient political system when compared to the complexity of social reality and other systems. States, thus, are pieces of machinery that oversimplify the variables of reality and are sustained also by illusions and promises.

So far, we have come to a critique of the place and the forms of representation of sovereignty. But a bitter taste remains: sovereignty seems to be where it always used to be. At the same time, it is everywhere. We live in a contingency where the previous authors brought up interesting contributions and critics when it comes to control and turn power accountable. But the existence of several streams to analyze and adopt a political position before the sovereign seems to embody a competition of many ideas. In this market of theoretical trends and solutions, one has to be careful to choose and interpret politics. In Richard Rorty, for example, knowing and thinking are not separated. Not all the methods are valid or share the same logic, but reason itself is ultimately a rhetorical matter (Rorty, (1979) 2009). In Rorty, there is no ultimate real foundation. To him, everything is temporary and there is no universal reason. Hence, Literature is perhaps more important for the rule of law than Philosophy. This importance is explained by the fact that, in Rorty, the best argument does not win, but the best story. Political commitment is not based on objectivity, but it hinges on shared narrative traditions. Like Foucault, Rorty takes into consideration how discourses are given. As in Literary critic, people make recommendations on the possibility of finding more illustrative theoretical examples and conceptions in an aesthetic sense and because a “definitive” justification is not possible (Rorty, 1989). Rather, people have to live with a plurality of proposals instead of being convinced that a certain political understanding is the only one and the best solution to tame power. Yet, this approach is not far from problems as not all the claims could be equally valid (in truth and logic). Furthermore, in our perspective, specific and universal criteria can be reformulated to understand politics and scrutinize power.

Thus, at the beginning of the 21st century, it seems that subjects are abandoned in a multi-narrative story which contains plenty of theoretical and political interpretations. In that case, we preferred to exhibit a multitude of political perspectives as a mosaic of alternatives instead of a source for disorientation. Each of those contributions is important to understand the justification and exercise of power. We need to be careful to interpret the Rortian

market of best stories in order to scrutiny sovereignty. From liberal, critique, post-structural, and post-modern perspectives, sovereignty has multiple adaptations and practices. As this brief epistemological history has shown, there are many paths and forms to understand power. Its multiform nature allows us to perceive its presence and force in many dimensions, from institutions to habits, people, sex, and language. However, when sovereignty acts, it cannot appeal to infinite reasons to justify its power. A circle must be drawn between the motivations and the outcomes of power, especially in state forms. Citizens, the governed, cannot accept all the precepts that sustain the actions from those who govern. The tension between governed and governors is what would define the final source and form of power. Therefore, this chapter will be complemented with the examination of the first condition that sustains governments: the issue of security. Security allows the initial ground to construct sovereignty and to enable the sociopolitical order. It summarizes the foundational moment or the exceptional creation of our political systems, as well as the governmentality or mundane moments that characterize societies. The next section examines the form to sustain sovereign power based on security. This constitution will take into account some of the above epistemological theories or political perspectives. In light of that, security motives will be analyzed in the construction of power and in the manners to administer populations. In turn, those manners would be crucial to examine surveillance and the attempts to restrain this realm via accountability mechanisms.

1.1.d. Constructing power: In the name of security

> *The reality of the events of September 11, 2001 and related actions intrude into our lofty conceptions of fairness, non-violence, avoiding harm to innocents, due process, transparency and the appropriate relationship between means and ends. A pragmatic survival ethos informed by notions of efficiency, prevention and turn-about-as-fair-play takes centre stage. Yet, as has often been noted, if in fighting our enemies we fail to be guided by anything more than pragmatism, we become less distinguishable from our enemies. Yet if we are rigidly guided only by the highest moral standards when opponents do not follow these, we may risk grave harm and even being destroyed* (Marx G. , 2004, p. 245).

From the previous section, sovereign power is no longer understood as a fixed and sacred political domain. Despite its multiple connotations, when it comes to analyzing sovereignty alongside governmentality and exceptionality, one characteristic arises amidst others: security. In this section, rather than charting the historical evolution of security as a concept, we address security as a practice that allow to construct power. Security is what allows founding and generating

politics. Security justifies the coup d'état and sustains the raison d'état. On security grounds, the very existence of the sovereign and the administration of populations is possible. In both actions, security is important to increase the authority regardless of its coercive aspects and repressive mechanisms.

In that sense, security institutions and practitioners are very pragmatic to interpret their world. Most of the time, security is understood as a relation of power mediated by real interests to consolidate the autopoiesis of sovereignty. For example, an intelligence analyst who works for a super-power, motivated by its formation and by a sense of patriotism, probably would focus her work on international security issues, such as the rise of China, Russia, and India. Another concern could be to improve the current strategies used to identify the radicalization of terrorism suspects inside the national territory. The list may continue in actions such as monitoring rival states and groups that use tactics in cyberspace, protecting an embassy from diplomatic interceptions that affect sensitive information, and so on. That is, analysts work according to the principles of realism, in which politics is a chess game that has already started and where the rules are dictated by an 'anarchic' international order. Security, in realism, serves as a mechanism of stability in a world of unpredictable threats. Intelligence services, like the Spanish "National Center of Intelligence" (CNI), are to protect the territorial integrity and the interests of the Spanish state. In the same way, the "Brazilian Intelligence Agency" (ABIN) has no legal authority to deploy espionage tactics that affect citizens' rights, giving the implicit assumption that Brazilian people must not be worried about governmental surveillance. Even if those roles are debatable, realism gives the idea that security agencies are focused on imminent threats to the extent that they have "few" time and energy to reshape their institutional practices and transform the world in the long-term. In the realism stream, policies must be efficient to implement feasible security measures. Having ethical and accountable principles is also important but these issues seem to be subordinated to realism in politics. However, security practitioners should know that realism is just one piece in the puzzle, one movement in the chess game. Other security approaches are as important because they present different connotations beyond the "visible" and short-term mandates analyzed by realism. Moreover, security limited to realism abolishes a set of possibilities that can improve the security practices that affect practitioners and the rest of society. In that sense, the following quotation shows perfectly the limitation of real politics and the necessity to compensate it with other security dimensions, especially from normative dimensions:

> At the beginning of the war, I believed fiercely in the brotherhood of man, called myself a follower of Gandhi, and was morally opposed to all violence. After a year of war, I retreated and said, Unfortunately nonviolent resistance against Hitler is impracticable, but I am still morally opposed to the bombing. A few years later I said, Unfortunately

> it seems that bombing is necessary in order to win the war, and so I am willing to go to work for Bomber Command, but I am still morally opposed to bombing cities indiscriminately. After I arrived at Bomber command I said, Unfortunately it turns out that we are after all bombing cities indiscriminately, but this is morally justified as it is helping to win the war. A year later I said, Unfortunately it seems that our bombing is not really helping to win the war, but at least I am morally justified in working to save the lives of the bomber crews. In the last spring of the war, I could no longer find any excuses.
> […] During the years I was at Bomber Command, my wife lived in that house [in enemy territory where I used to drop bombs]. She was still a child. The nights when the bombers came over, she spent in the shelter. No doubt she was sitting there the night [of the bombings]... (Dyson, 1979, p. 64).

As Dyson shows by his real experience during the last World War, humans can be transformed when they are merged into real politics, and even in the worst conditions, they can believe that they execute goodness or are not evil. However, since real politics and the rules of the international "anarchic" order are not separated from people of flesh and bones, security is not just protection and the search of legitimate results for the safety of people, either by good or bad means. Security is also a governmentality process that is not separated from rational, normative, institutional, and even symbolical, irrational, and informal practices. Being a soldier is not only being a defender, but it is also being a warrior, a potential saver, a potential destructor, in short: it is just one piece inside big political machineries. In this kind of apparatus, security is managed beyond realism, for instance, security can be also understood with parallel approaches from liberal, critical studies, and deconstruction/ securitization analyses.

In liberalism, Michael Howard defines "liberals" as all those "who believe the world to be profoundly other than it should be, and who have faith in the power of human reason and human action so to change it" (Howard, 1978, p. 84). But liberal theory provides much more than imagining a better world or a utopian project. Indeed, the international spread of liberalism has been considered the Western ideology related to the representative democracy as mentioned in the last section. However, different assumptions about human nature separate classical revolutionary liberalism from later evolutionary liberalism. In *Rights of Man*, Tomas Paine noted that "man […] is naturally the friend of man and that human nature is not itself vicious" (Paine, (1791) 2011, p. 169). In this classic assumption, the democratic revolution would free mankind from corrupting influences and human reason would emerge to transform the world. To achieve this, Paine (1791: 230) was one of the first popular proponents of free trade as a means of promoting peace. On the other hand, for evolutionary liberals, there is a cautious view regarding human nature. Immanuel Kant, for example, depicted human nature as

“a mixture of evil and goodness in unknown proportions” (Kant, (1798) 1974, p. 181). But Kant remained optimistic about man's ability to evolve through reason. From both thinkers, what is at stake is that liberty is essential to every human endeavor. Moreover, security gains insofar peace is reinforced, and conflict is avoided. Transferred to contemporary security, reasonable people constructing reasonable institutions, applying reason, and respecting the liberty from other individuals would avoid deviations of power but also transform security practices on moral and ethical grounds. Here, the governmentality of populations is presented when security practices intervene to “tame” the future and to recover the linear sense of progress through statistical and rational calculations (Lobo-Guerrero, 2007), creating scenarios of preparedness (Collier & Lakoff, 2008), or risk assessment to avoid catastrophe and disaster (Aradau & Van Munster, 2007). Based on the ideas of Enlightenment and freedom, those examples are contemporary rational tools at the service of security that operates in a linear conception of progress to find or improve a situation of relative safety and unnecessary conflict; reshaping even immediate realism in politics.

For critical studies, meanwhile, security is not given a priori and cannot be implemented ignoring an overall context in which political interests encompass its functions and results. Having equality and freedom as starting points, critical studies are related to the continental philosophical tradition. In this group, the literature on emancipation (Rancière, 1999) (Badiou, 2014) is concerned about the security shifts that endanger civil and political rights –though one must admit that this concern was shared with Liberalism. Rather than conceiving order and security practices in the way that many scholars of realism have done, this stream challenges how security constitutes communities and governs populations. For example, in the question of securitized borders, according to Rancière (1999), the denial of mobility to large parts of people in the world – illegal immigrants, refugees, asylum seekers, economic poor migrants- is one of the most significant obstacles to equality in our time. If in realism those people might be considered as threats to security, in this stream, the answers of security can be a threat to more equality and justice for everybody. Thus, thinking of equality as a starting point to interpret social and political relations can help to unmake the hierarchical logic that security entails, while, at the same time, it can help to furnish a new relationship with the “other” (Aradau & Blanke, 2010).

Another example of critical studies comes from the mentioned theory of the state of exception by Agamben (1998). This reformulation has added two important points in this stream. The first is that security is an exceptional practice that draws boundaries between political life (bios) and abject, disqualified, or bare life (zoe). Not only the state of exception produces sovereignty and political community, but it also reflects the image of bare life, i.e. life that can be killed with impunity. Based on the Schmitt concept of sovereign presented before, Agamben (1998) affirms that 'bare life' is the original gesture of sovereignty and points out

to ways in which sovereignty is constitutive of disgusting politics. In a state of exception, where the sovereign is exempted from all legal rules, subjects no longer enjoy the protection of the legal order. Bare life is the point of internal exclusion enacted by sovereignty; it is a life that is not set outside the political order but remains included as exclusion. The state of exception is explicitly linked with fascism in Agamben's work, but this raises questions about the forms of disgusting politics of security deployed by contemporary democracies as well. Agamben's legacy has fostered analyses of the so-called "war on terror" and contemporary security policies. The war in Iraq (Diken & Laustsen, 2005), refugee camps and airport holding zones (Salter, 2008), humanitarian intervention (Weiss, 2016), detention centers for terrorist suspects (Cole, 2009), have all been recognized as exceptional practices in which the life of some people is reduced to that of bare life. However, as expressed in the second section of this work, taking exceptional spaces and performances disconnected from normalization trends would be a mistake. Even the most exceptional measures are attached to governmentality components. Even the detention center for terrorists in Guantanamo Bay was constituted by administrative rules and regulations (Johns, 2005). Rather than constituting empty spaces of 'bare life', camps and other exceptional spaces are governed through bureaucratic technologies and regulations which offer valuable clues to scrutinize security measures.

The last general stream associated with security studies is deconstruction/securitization. The separation of this stream from the previous one is controversial as the reader might consider deconstruction as part of critical studies and securitization as a trend that not necessarily aims to deconstruct security practices. In this work, they are put together because both deconstruction and securitization share this same idea: to reexamine the discourses, motivations, institutional procedures, and heuristic mechanisms that are taken for granted to deploy security measures according to the sovereign intentions. This reexamination exposes the contradictions, limits, and possibilities for security practices. This stream is not free of critiques as it will be attested below. But considering that this work has to examine surveillance assemblages attached to security and beyond and they must be deeply reconstituted for the sake of accountability principles, deconstruction and securitization will serve us to depict and understand security. To do this, first, we will return to the origins of security as a fundamental part of the social contract which supports the sovereign authority in the form of state. Once this authority is constituted, security will be analyzed as a right, then as a good and finally as an ending-goal to fulfill the expectations of the social contract to secure people.

Going back to the beginning of the Modern era, security is introduced by the very transformations of politics after the Renaissance era in terms of religion, rule, and secularized power. Since those times, if sovereignty finds no more a primary foundation in external causes (in God and the authority of tradition), it is necessary

to justify its pre-eminence through the exhibition of what allows its existence: only the sovereign can ensure in a visible and incontestable way a situation of peace that avoids civil conflict. In a context in which the state has no moral and religious mission, as it is no longer submitted to the service of the Church, and as it gives up the mission of taking care of souls, the state started to assume the secularized administration of people. Security seems to be imposed as the residual purpose of politics in a world that has stopped waiting for the state to be involved in the virtue and salvation of citizens (see the previous section). Since then, the state has taken the duty to ensure the population. At least, it has promised to accomplish the biological integrity of people.

Notwithstanding, even when the state is reduced to the imposition of commanding rules and understands citizens as subjects of obligations, authority is not exercised in an automatic sense. In Hobbes, for instance, the security provided by the state is not sufficient to justify the transference of rights from individuals to the sovereign. According to him, there is an authorization process of delegation of rights –such as the act to be represented, to speak, and to act according to the people- which is given, not delegated, to the sovereign. In this sense, the actor [the state] acts by authority; the state is legitimate if acts on behalf of the citizens, who are the virtual authors. Hence, the definition of the social contract, which authorizes and grants the right to govern by transferring authority to an assembly, to a council, or a man, is accomplished insofar as the rest of individuals do the same (Hobbes, (1651) 2016). Therefore, a judicial value is given to the authority of a representative entity. In that sense, for Hobbes, we are witnessing the emulation of the public will, and the consequences of that emulation are repeated since then. Even in the Absolutist version, the modern state of the 16th and 17th centuries is conceived as an agent whose authority is built, from the beginning to the end, to consider the people. Since then, legitimate politics no longer emanates purely from any entity outside the will of men. In short, the consent of citizens is the very source of state authority. Even in non-secularized states in current times, the divine right is not sufficient to conduct politics.

Hence, the authorization of authority by people, the source that enables sovereignty and security, is expressed by Hobbes as follows:

> And because such arguments must either be drawn from the express words, "I authorize all his actions," or from the intention of him that submitteth himself to his power (which intention is to be understood by the end for which he so submitteth), the obligation and liberty of the subject is to be derived either from those words, or others equivalent, or else from the end of the institution of sovereignty; namely, the peace of the subjects within themselves, and their defence against a common enemy […]. And law was brought into the world for nothing else but to limit the natural liberty of particular men in such manner as they might not hurt, but assist one another, and join together against a common

> enemy (Hobbes, Leviathan (Longman Library of Primary Sources in Philosophy)., (1651) 2016, pp. 133, 164).

Despite the permission given to the sovereign, there is a difference between authorizing the sovereign to regulate a sociopolitical order on behalf of the people and the very execution of sovereign power. If the authority of the state increases its power, the authority can only give credibility to its power by obtaining confidence and trust from those who are submitted to it. For individuals, this implies the conviction that their political existence is inseparable from obedience to the law. The need for authorization is based, then, on the legal fiction that operates the transformation of the subject into a citizen. A state based only on the monopoly of violence would not be fully sovereign since it would obtain its legitimacy through the fear of men. The authority of the state weakens each time it appeals to the imminent menace of the state of nature, the situation of a war of men against men. Hobbes does not ignore such a menace, but what really bases the construction of the state to him is the transference of authority from the author (the people) to the actor (the state) as a political model capable of avoiding the radicalization of conflicts and the civil war (Hobbes, (1651) 2016). It is clear, therefore, that the objective of security is not sufficient to ensure the legitimacy of sovereignty in the hands of the state, but it is a necessary precondition. The dispute, therefore, between those who affirm that security is not a sufficient condition for political authority –security per se cannot legitimize authority- and those who support security as a precursor or an indispensable element for public authority –security can be legitimate since it allows other values- is a debate that continues even nowadays.

In the latter interpretation, security can be understood again in terms of realism: security is the first right. Security is the first of rights because, as Michaël Foessel claims, its primacy must be understood not only on the descriptive level (without security, there can be neither freedom nor equality) but also from a normative point of view (since all rights can be reduced to security) (Foessel, 2011). Security is efficient insofar as it allows reformulating the fundamental rights of individuals: liberty is, for example, the guarantee of a peaceful existence; property, the right to use one possession without usurpation; equality itself finds its first expression in fear of violent death and in the egalitarian desire to overcome it (Foessel, 2011). Whether security and liberty establish a dialectic relationship rather than a non-zero-sum game, is not the point now. The point here is that without a minimum level of security other rights can be barely demanded. Of course, this analogy from the Modern era must be taken cautiously to the present time, as liberty rights must not be obliterated in the name of security. But at the end of the day, the conditions to liberty depend on the very conditions in which security is provided and administered.

Those conditions can be depicted if we understand that security is also the first good. Security as the first of the goods consists of defining security not as a right, but as a value to be provided by the sovereign to the people. It consists of making security as the horizon of what is desirable to people (Foessel, 2011). Delivering security as a good implies in "measuring" the forms it is implemented and supplied to the people. Historically, the delivery of this good appears in the eighteenth century, at the moment when, as Foucault affirms, insecurity and war were no longer "inevitable misfortunes" related to divine punishment, to bad luck, or the nature of man (Foucault, (1979) 2008). Insecurity became a social problem that could be evaluated rationally. In this perspective, it is possible to talk about the cost of crime, where the crime no longer refers only to a criminal offense, but to the inequalities that permeate every society. It is also the moment in which contemporary concepts such as the "police" arise. In Foucault, in the perspective of the police, the problem of insecurity no longer refers to the founding moment of the social contract, but to an everyday task of providing security and stability to governments, then to the people. Thus, the de-dramatization of the problem of insecurity has been fully realized in the field of the police. The matters of the police belong to the politics of every day (Foessel, 2011). However, the police tasks never are disconnected from the foundational moments of the sociopolitical order and the origins of this institution. In our vision, the problem of insecurity has passed historically from an exceptional-normalization category towards a normal-exceptionalism one. In other words, traditionally, the police are a power linked to governmentality, delivering security as a good and maintaining a certain distance (though it is not disconnected) from the original foundational security principle (security as the first right that sustains the social contract).

However, at present, we are witnessing the opposite movement: the expansion of insecurity and fear. The problem of insecurity, even when it is not simply the antagonistic term for the lack of security, is moving from exceptionalism to normalization. This movement is explained insofar as there is a modification in the concept of security, as it started to differentiate from the social contract and became an "ending goal". Security started to reproduce *just* security. It enhanced its banalization. This happens when security, which stills operates in a generative and generating logic to preserve the social contract, concentrates the list of expectations that a legitimate state must deliver to the people. One consequence, then, is the securitization that the world is experiencing nowadays and here we return to the securitization stream. In that change, there is no political discourse or electoral program that ignores security. Security constitutes a priority and a set of values that cannot be explicitly confronted. No candidate, party, or citizen is openly positioned in favor of dismantling security or is contrary to secure people against old and new threats. Politics has become the management of all kinds of insecurities, a movement of expansion that anticipates threats and dangers that abound.

Even civil society institutions and international organizations such as United Nations have proposed, with good intentions, to cover basic human needs and individual rights with the label of "human security" (MacFarlane & Khong, 2006). Yet, the problem of this new approach to security, on the one hand, is that it turns security into a good that must be provided every time and to everybody. On the other hand, it securitizes all experiences of deprivation and injustice. Given the profusion of social, environmental, and economic crises, among other threats, it is tempting to refocus the political attention on every single person in order to reconstruct the social contract in the 21st century. As the subject of human security is the biological subject facing transnational risks and catastrophes, then, the range of threats for this subject is practically unlimited: "The feeling of human security consists in a child that does not die, a disease that does not spread, a job that is not suppressed, an ethnic tension that does not degenerate into violence, a dissident who is not reduced to silence" (MacFarlane & Khong, 2006, p. 23). Human security, then, tends to naturalize the list of topics established for security. However, political action presupposes a hierarchy of threats instead of equalizing them around a vital subject worthy of protection, especially when institutions and policing are put into the equation. Securitization and de-securitization studies have already addressed those hierarchies extensively as well as the criteria to select certain issues upon others in the name of security (Balzacq, 2011) (Bourbeau, 2014) (Yauri-Miranda, 2018).

In addition, the banality of security also relates to critical situations, such as terrorist attacks, and diseases and pandemics. Nowadays, individuals are aware that there is nothing natural about security and that everything on it is political even if threats come from nature. Sometimes, these critical moments constitute a great justification for the edition of norms. But as seen above, due to the exceptionality and normalization categories of sovereignty, the new security measures must be understood as reactions to normalize the administration of populations. Security as an ending goal or the banality of security is based upon the equivalence between the expectation of safety and the answers to achieve it. This banality, for example, is observed in national security as this is not circumscribed anymore to sacred and supreme threats afflicting a state and its population. National security melts and moves towards other areas, such as enforcement, digital infrastructures, and mundane routines of people. In that sense, Foessel (2011) mentions that the night errant should thank security managers for allowing a quiet walk at night under the stars. To him, this experience is as political and significant as war itself because both depend on the normalization of security measures. The walker must thank the sovereignty for the deployment of rules that combat fear and different threats. At the same time, the walker at night must forget those same mechanisms of power, as if they had never existed.

Security measures interpret fear as the natural cause of the developments of security and surveillance. Both the security practitioners as well as the audience

that security seeks to convince might understand fear as the source that legitimizes the implementation of answers and measures. This understanding is limited as the sources of legitimacy are not threats, by the authorization of sovereignty by people affected by the same threats. This slight differentiation, present in the Hobbesian social contract, is extremely important in order to construct answers against fear. For instance, whereas fear was the anthropological origin of the social contract, the deployment of contemporary security and surveillance assemblages can use other connotations to understand fear.

Hobbes ((1650) 2010) distinguished between feeling "fear" and "being frightened" by the fact that the former entailed a rational act that encouraged men to draw conclusions about their state of fear, uniting them against it. The latter consisted of escaping from what was perceived as a threat. Here men do not seek to control the danger but they wish its disappearance. Thus, what is common to different cultures, political preferences, and states is that all of them share diffuse threats. Yet, the current answer to fear is given in the sense of “being afraid”. In times when the state no longer convinces about its capacity to guarantee the social contract delivering security either as the first right or as the first good, individuals sometimes are left alone to their frightening threats. And when the security apparatus reacts, many times it moves on a ground marked by anxiety and preemptive paranoia.

Many times, security sees the delinquent, the marginal neighbor, the clandestine immigrant, and other figures that might cause disorder as elements for control and dissuasion. The borderline between the normal individual and the transgressor moved in the sense of encompassing exclusionary practices at different intensities. Studies on exclusion, either through physical walls in politics of imprisonment (Wacquant, (1999) 2009), or in symbolic walls separating virtual communities which are polarized in their beliefs, prove the different scales to exclude and create social segmentations. But despite we share common threats; we refuse to feel the first kind of fear that incites cooperative actions to reconstruct the Hobbesian contract. The paralysis and lack of a common answer are explained insofar as we are never truly equal before the threats that loom over the world. If there are "globalized risks" we do not see ourselves inserted in a voluntary community but as atomized individuals living in fragmented spaces that ensemble the “ecology of fear” (Davis M. , 1998) and segregation and crime as in the “city of walls” (Caldeira, 2000). This sensation of fear has increased the differentiation of spaces reserved for the unwanted and for those people that minimally pose a threat against security, from the people that constitute targets for the actuarial criminology to the increasing predictive nature of surveillance that watches everybody.

For sovereignty, those targets represent dangerousness. Dangerousness is understood as the potential harmfulness posed against the security of other

individuals or to the entity that implements sovereignty. In this regime, the identification of the individual profile is inseparable from a prediction about his/her future behavior. The concept of dangerousness is not new; it was introduced at the end of the 19th century by Italian jurists of the positivist school of law. At those times, it was linked with a certain conception of progress and a strong belief in the powers of technical expertise to tame the future. Nowadays, the concept has returned by the anthropological pessimism and distrust of the therapeutic function of rehabilitation. Evaluated by the risk manager, dangerousness is performed according to a probabilistic logic that can only be confirmed *a posteriori* by the failure of the penal system and by recidivism of offenders. This explains, in part, why we are potentially "dangerous" persons for surveillance dispositives such as video cameras and checking points (Foessel, 2011). The indiscriminate suspicion resembles the banality of security and has "no limits" to expand the power of the gaze(s).

Because of those characteristics, the model of aversion seems more appropriate to designate our current response to threats rather than the classical Hobbesian fear that allowed the social contract. Challenged by diffuse dangers, imagined or constructed (Yauri-Miranda, 2018), there is a wish to expel the threats from the world even if there is no concrete solution to them. As repulsive and disgusting objects increase, securitization expands and is also demanded through disgusting methods. Faced against risks that are not limited to a single issue, to a concrete group or one country, the "illusion of politics" proposed by Luhmann a few decades ago reacquires force, especially in our times. While danger is everywhere, the world itself represents danger. Fear has lost its capacity for circumspection and has created a sensation of anguish. In short, it seems that expectations cannot be longer circumscribed to a controllable horizon of expectations. The risk society postulated by Ulrich Beck has been internalized not to understand risks themselves, but to assess, quantify, and tame the side effects of securitization and war (Beck, 1992). The current fears bring up distress, and for this reason, they no longer allow us to constitute a common world. Hans Gumbrecht mentions that even the chronotope that marks the rhythm of historical evolution has stopped, crystallizing a present that encompasses past ideals and a future that cannot be entered or crossed (Gumbrecht, 2014). The past represents the ideal situation of safety, and the future withholds the amplification of fears and threats. In that sense, we live in a spacetime of paralysis where dangers abound.

These times demand to reacquire the right to feel "fear" without being "frightened". Catastrophe discourses expand and operate like self-fulfilling prophecies that raise anguish and avoid solutions to threats. Fear, as expressed by Foessel (2011), needs to create a common action that is only possible where there are public institutions and a common world, as Hannah Arendt would say. Creating that world consists partially in observing how individuals react to the banality of security and how they can change it.

When it comes to change security in a context of the banality of this value - where major changes are exemplified by the development of risk assessment, crime prevention, community safety, private security, and mass surveillance- one important question is: how much security must be deployed and in the name of what? Lucia Zedner, argues that this question consists in thinking more critically about security than its promoters might like (Zedner, 2003). Thus, security needs special justification and it is necessary to develop guiding principles in order to regulate its procedures and effects. In turn, this leads to the larger question of whether and in which manners is possible to regulate the banality of security in order to ensure accountability, fairness, and inclusive provision of protection.

This section has examined the last form of sovereign power. Based on the construction and promotion of security, this value can be interpreted as the first right, good, and process. However, the forms to promote security are adapted according to the interpretation of fears. Trapped in a vicious circle of the banality of security, in which this value interprets fears and threats everywhere, and as the social contract is modified in the name of fighting diffuse and global phenomena, the sovereign might deploy dispositives of governmentality to administrate populations and to replenish exceptionality within the sociopolitical order. In that sense, if security is the "father" of the reasons that sustain sovereignty, surveillance is the "son" that inherited many of the security procedures to handle suspects and validate people. Surveillance amplifies and redefines security trends, as it can be considered as the specialization field to administer populations and regulate individuals through observation. The next sections address the ideas behind surveillance, privacy, and accountability. Those ideas, in turn, will serve to structure and operationalize the analysis of specific cases in this study.

1.2. On surveillance: Real metaphors and perspectives

> *They [the Mehinacu Indians of Brazil] can tell from the print of a heel or a buttock where a couple stopped and had sexual relations off the path. Lost arrows give away the owners' prize fishing spot; an ax resting against a tree tells a story of interrupted work. No one leaves or enters the village without being notices. One must whisper to secure privacy - with walls of thatch there are no closed doors. The village is filled with irritating gossip about men who are impotent or who ejaculate too quickly, and about women`s behavior during coitus and the size, color, and odor of their genitalia.* (Marvin, 1977, p. 32).

As shown in the above paragraph, "being" or "existing" to other eyes is perhaps the awakening act, the moment of consciousness per excellence even in the tribe. Love, conflict, and many feelings depend on how we look at the world of concrete and abstract things. Painters and photographers do this work of observation and translation very well. For instance, during the romantic era, painters depicted scenes in a more scientific approach like in *Wivenhoe Park* by John Constable (1816), or in an emotive approach condensing a feeling like in *Monk by the Sea* by Caspar David Friedrich (1810). Since the first devices to capture light and take photos to the Instagram era, visibility and exposition shaped the forms to frame reality and interpret other people.

Seeing is not necessarily a contemplative act. For example, staring at others was deemed as an act of robbing freedom and identity. In Jean-Paul Sartre's words, "while I attempt to free myself from the hold of the Other, the Other is trying to free himself from mine; while I seek to enslave the Other, the Other seeks to enslave me... Conflict is the original meaning of being-for-others" (in Yar, 2003, p. 259). From love to conflict, if the gaze is the first act of meaning, of constituting someone's identity, then surveillance is the act of giving meaning to people and identifying someone by deploying multiple gazes. Either for banal or deeper reasons, surveillance is watching and giving sense to our reality. Avoiding permanent eye contact with strangers while traveling in public transportation or fixing our mental attention to this text, both constitute a preemptive act of surveillance. Thus, surveillance, more than a fixed concept is an attitude, a way of interpreting and being interpreted by other person or audience.

These interpretations, in turn, can be mediated by different senses, interests, and technologies. The conflictive interpretation of the gaze, as expressed by Sartre, is entailed because politics is a sphere of power, a domain where cooperation and competition interact to regulate social life. If humans are political animals and live in society, the array of gazes define the multitude of people. The

act of watching common patterns and behaviors are as important to politics as to the very individual concerned with her/his position, past, and future. And if we are to scrutinize surveillance, it is essential to understand how surveillance is used to govern populations in a certain time and place. In that sense, surveillance is related to crucial metaphors such as the panoptic.

The panoptic, the full observation, is a metaphor of the panopticon building designed by the utilitarian philosopher Jeremy Bentham in the 18th century. As a product of rationalism applied to the old penology, the design of the panopticon consists of a penitential circular structure with a watching house at its center, from which the inspectors of the institution are able to watch the inmates. At the same time, the inmates, located in cells at the circular borderlines, are unable to see the watchers. The panoptic gaze, therefore, embodies the pathological approach of controlling in a continuous and intrusive way. This gaze is supposed to mitigate inmates' deviations and internalize satisfactory behavior rules defined by the watcher.

In that sense, the panopticon, as a physical structure, became a metaphor for surveillance in different contexts. For example, in the famous novel *Nineteen Eighty-Four*, George Orwell describes the perpetual war between Oceania, Eurasia, and Eastasia, the superstates that emerged from a global atomic war. In this reality, the sovereign power is the "Big Brother", an absolute panopticon which controls the citizens of Oceania by violence and coercion (Orwell, (1949) 2009). Orwell, at those times, alerts the readers about the perils of omnipresent surveillance which assembles totalitarian and authoritarian states. Another example is the novel *Moscow 2042* by Vladimir Voĭnovich. This story narrates a soviet time traveler who finds out how the new leader, Genealissimus, has achieved the socialist utopia in Moscow. Yet, in this future, economic poverty persists and obedience is enhanced according to the hard and soft power established by the leader in a society that degenerates to corruption and autocracy (Voĭnovich, (1986) 1990). In that sense, both novels are examples of dystopian surveillance societies, presented in the form of tragedy in the West and satire in the East, respectively.

Both fictional stories are valuable cultural and historical sources to understand each writer`s time. They also could be deemed as cases for an exceptional panoptic machine that establishes different mechanisms of surveillance of populations. However, panoptic surveillance also belongs to governmentality, to the normal moments beyond exceptional circumstances. In this logic, many of Foucault's concepts –, discipline, regulation, the biopolitics of population, discourses of security, and governmentality – are indeed a work stemmed from his critical analysis of the panoptic throughout western history. In *Discipline and Punish*, Foucault outlined his general project as a "history of the modern soul and of a new power to judge; a genealogy of the present scientific-legal complex from which the power to punish derives its bases, justifications, and

rules, from which it extends its effects and by which it masks its exorbitant singularity". (Foucault, 1975, p. 23). In that sense, Foucault argued: "the major effect of the Panopticon was to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" (Idem, p. 201). As Foucault pointed out, there is no need for the inmates to be actually watched; what was important was that they did not realize the precise moments they were watched. The self-disciple represents, thus, the normalization of sovereignty, the administration of population through internalized habits of everyday surveillance. Surveillance first lesson in Foucault is the continuous characteristic of monitoring, the implicit/hidden power source of the watcher; and the self-discipline of the watched.

Although Foucault wrote and spoke about the gaze, Gilbert Caluya reminds us that this should not be taken as an analysis of the gaze, but an analysis of power *through* the use of the gaze. The gaze is only important insofar as a concrete mechanism through which power is exercised. "The principle of the panopticon is not the gaze but the automatization and disindividualisation of power" (Caluya, 2010, p. 626). In this perspective, Foucault concluded that power is not present entirely in a person, in an institution, or bureaucratic arrangements. These examples are just mechanisms whose internal logics produce the relation in which individuals are inserted and power is conducted and transformed. Power has a subterranean characteristic which is allowed by those mechanisms but is not circumscribed to them. In sum, while Jeremy Bentham's panopticon is a penal building, Foucault's panoptic is a machine of power that can be applied to extra-penal spheres. "Is it surprising that prisons resemble factories, schools, barracks, hospitals, which all resemble prisons?" was a metaphorical remark formulated by Foucault (1975, p. 309). The panoptic, the surveillance machine, thus, can be adopted in several domains and practices. All contemporary institutions subject their members to forms of bureaucratic surveillance. Individuals with different financial records, education, and lifestyles come into contact with different institutions and hence are subject to a sort of panoptic:

> At the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building; they have two windows, one on the inside, corresponding to the windows of the tower; the other, on the outside, allows the light to cross the cell from one end to the other. All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light the small captive shadows in the cells of the periphery. They are like so many cages, so many small theaters, in which each actor is alone, perfectly individualized and constantly visible (Foucault, 1975, p. 200).

From Foucault studies on the panoptic, two main ideas remain; the panoptic consist of a machine of power where the few observe the many whereas the latter internalize a top-down discipline; and the panoptic is a machine that explains the microphysics of power –the microscopic relations of power in every social organization. Both ideas will be questioned in an intense theoretical discussion after Foucault's death in 1984. Whether surveillance can be analyzed through the panoptic metaphor is a question opened to several interpretations even nowadays.

On the one hand, some scholars believe that technological developments, especially the rise of computers and digital data networks, demand an updating of the panoptic metaphor. For example, Mark Poster coined the term "superpanopticon" to describe the huge collection of information by surveillance recipients as we create bulky amounts of data (Poster, 1990). Diana Gordon, in turn, suggested the term "electronic panopticon" to understand the new digital technologies of surveillance in the late 20th century (Gordon, 1987).

On the other hand, further studies support a vision through which we can dispense the panoptic idealization. Thomas Mathiesen, for example, agrees with Foucault's genealogy that identifies the change in the forms of punishment (from torture to imprisonment), the change in the content of punishment (from the body to the soul). However, he inverts the panoptic idea where the many see the few to the situation where the few see the many. To him, Foucault failed to take account of the rise of the spectacle in mass-mediated societies where the many watch the few (Mathiesen, 1997). This new situation, called "synoptic" or "synopticon", became the new metaphor to analyze surveillance in contrast to the static, unidirectional panopticon (Wood, Ball, Lyon, Norris, & Raab, 2006).

Other arguments in favor of reformulating the concept of the panopticon are summarized by Roy Boyne in *Post-Panopticism*. This scholar identifies three bullet points to support his vision: a) there is a displacement of the discipline panoptic ideal by mechanisms of seduction. As individuals are attracted and feel comfortable to be watched, there is a redundancy of the panoptical demand of self-surveillance to constitute the normal 'Western' subject; b) there is a reduction in the need for panoptical surveillance on account of simulation, prediction, and action before the fact, exemplified by the normalization of habits and accepted behaviors; c) there is a supplementation of the panopticon by the synopticon as the latter is more effective to control and to produce reliably docile subjects (Boyne, 2000). He concludes that the panoptical logic is not simply being eliminated insofar surveillance can also work through the panopticon concept. However, he argues in favor of changing the sites of its application and recognizes the limits of that concept especially when it is confronted with the synopticon metaphor, where the many see the few.

The synopticon concept also implies controlling and producing docile subjects by traditional ideas of amusement, seduction, and chaos emanated from sovereign powers. In that sense, fictional Literature again offers two paradigmatic examples. The first one is the dystopian novel *Brave New World* by Aldous Huxley. Written in the depression era, this novel can be considered a contestation against the utopias of those years. Huxley narrates a free-pain society where socially accepted behavior and amusement result from a strong social cast stratification and from the consumption of a licit drug: *soma* (Huxley, (1932) 1998). Instead of the iron fist of a ruler like in the Orwellian reality, social control here is exercised by a series of rational tools. The internalized discipline of the many is found in a spectacle mass society opposed to the "savage" and "unhappy" habitants who live at the fringes of the World State. In this state, the social order brings happiness but at the cost of artificial feelings and mass distractions. The second example is the famous novel *The Trial* by Franz Kafka. This is the story of Joseph K., a man who is arrested but does not know the details and the reasons for his prosecution. The trial is different from regular legal proceedings as bureaucracy is secret, from the charge, the court rules, to the judge identity. The attorney promise to elaborate a judicial brief, but since the charge is unknown and the rules are secret, no information is really given to K. The story is a psychoanalytical symbol because its environment is permeated by a fantastic and dreamlike world, as in the encounter with a priest in a cathedral where K needs to confess crimes he cannot remember (Franz, (1925) 2015). Besides, this story can be considered as a sociologic criticism of the rational and inhuman Weberian bureaucracy as K is just one victim of a technocratic judicial labyrinth.

Likewise those novels, the synoptic metaphor also is linked with characteristics that would serve to keep the masses in a state of distraction and relative chaos. This is explained by the fact that the machinery of surveillance is potentially at the service of the watched, the crowd, as much as of the watchers. To Boyne, for example, the aspirations to one-eyed total surveillance have been displaced by technological and strategic developments, rendered unnecessary by relatively efficient continuing socialization into self-surveillance and auto-seduction, like social networks and the Internet 2.0. These tools have exacerbated the role of the mass media, and, in the words of Boyne, have shown, in any event, the failing attempt to actualize surveillance in "quasi-total institutions" (Boyne, 2000, p. 302). In our view, Boyne is correct refusing the idea of a centralized watcher, but the Foucauldian panoptic is still valid as it was never a matter concerned with centralized gaze, rather it consists in how the gaze(s) serve as the mediator(s) for surveillance according to the principles of the microphysics of power; the fragmented social domains where power is transformed beyond institutional borderlines. Surveillance was never deployed by centralized and unilateral surveillers even in fictional stories.

Huxley and Kafka´s dystopian examples are not necessarily opposed to the panoptic surveillance metaphor. Indeed, they shed light upon new domains and mechanisms that are familiar to surveillance. The tough social control or hard discipline is complemented not only by the synoptic metaphor but also by broader social changes. Proof of these changes is given by Zygmunt Bauman. For him, most of us are socially and culturally trained and shaped as sensation-seekers and gatherers, rather than producers and soldiers as in the old disciplinary societies. Because of that training, "Constant openness for new sensations and greed for ever new experience, always stronger and deeper than before, is a condition sine qua non of being amenable to seduction" (Bauman, In search of politics, 1999). In *Liquid Modernity*, he describes the disintegration of the heavy institutional structures of industrial modernity, and the emergence of new fluid and transient forms of sociality in their place (Bauman, 2000). Central to this transition is a process of individualization, whereby powers previously assumed by the state or institutions such as class or the family are devolved downwards to individuals. Making the individual responsible for his/her self-supervision and the only anchor of collective actions implies no stable ground in which to root a human life-project. Everything is transitory, shapeless, and liquid such as the friendship concept managed in social networks like Facebook. Bauman, thus, affirms that this kind of individualization represents the transition to a post-disciplinary or post-panoptic society where traditional discipline no longer dictates broader social changes.

Bauman understands the Panoptic as the metaphor of totalitarian regimes, where there is "no private space; at least no opaque private space unsurveilled or worse still unsurveillable" (Bauman, 1999, pág. 49), while in the synopticon all spaces seem to be overrun by personal and private lives. Bauman argues that instead of being subject to disciplinary surveillance or simple repression, the population is increasingly constituted as consumers and seduced into the market economy (Bauman, 1992). While surveillance is used to construct and monitor consumption patterns, such efforts usually lack the normalized soul training which is so characteristic of panopticism. For him, the monitoring of market consumption is more concerned with attempts to limit access to places and information or to allow the production of consumer profiles through the ex-post reconstruction of a person's behavior, habits, and actions. However, in our vision, the panoptic does not work only in totalitarian or closed regimes. Since the panoptic is a machine of governmentality, and because governmentality cannot be separated from exceptionality political decisions, the panoptic is still valuable in other kinds of regimes and sociopolitical orders. Moreover, market practices limit access to places and information according to their principles but they do this work in a substrate of disciplined bodies that are to fulfill commercial expectations and behaviors. This becomes clear in advertising based on social network content and mass data analytics that address the best targets and profiles to consolidate consumption patterns. In addition, those tactics represent the absolute

convergence among different technological mechanisms, commercial strategies, and "passive" personal data souls. Therefore, at the end of the day, the panoptic is diluted but still survives the so-called transition to a liquid post-disciplinary society.

Another type of post-disciplinary society that serves to analyze the recent evolution of surveillance was coined by Gilles Deleuze in his *Post-Scriptum on Societies of Control*. In this short essay, he gives an account of the shift from discipline to "control societies" in which the post-industrial transformations of production and consumption have altered the panoptic principles (Deleuze, 1995). In Deleuze, the question is not of the fixity of institutional structures such as the prison or even the state but of mobile forms of surveillance that can track or fix 'dividuals' (nomads defined not by their right to be individual or by their intrinsic worth but by the systemic process of coding that differentiates one member of a population from the next) in real-time and space (Ganesh, 2016). Discipline still exists but it is no longer attached to fixed institutional spaces – from prisons to mad-houses to schools and so on– but to new mobile and flexible techniques of power that serve to "ultrarapid forms of apparently free-floating control" (Deleuze, 1995, p. 178). Indeed, Deleuze prefers modulation instead of discipline as a term to describe a social control that operates through mobility and speed. Deleuze writes: "Confinements are moulds, different mouldings, while controls are a modulation, like a self-transmuting moulding continually changing from one moment to the next, or like a sieve whose mesh varies from one point to another" (Idem, pp. 178–179).

By emphasizing modulation and mobility, "control society" goes beyond the panoptic metaphor to analyze further characteristics in contemporary surveillance. For example, surveillance extrapolates the gaze as a mediator mechanism that allows and guides the act of watching and being watched. Surveillance refers not only to the sphere of supervision but also to the collection of information, to the analysis and use of knowledge (Wood D. M., 2007) (Gandy Jr, 2012). The role of telecommunication providers and data managers, as well as the different technologies used especially after the advent of portable chips and the Internet in the last decades of the 20th century, allows us to understand surveillance in mediation terms, that is, it allows us to determine political players and strategic technologies adopted to collect and refine information (Lyon, 1994). For example, current software and computing are crucial points to deploy surveillance, as stated as follows:

> We set up a system at Pathfinder in which, when you visit our site, we drop a cookie into the basket of your browser that tags you like a rare bird. We use that cookie in place of your name, which, needless to say, we never know. If you look up a weather report by keying in a ZIP code, we note that. . . . We'll mark down whether you look up stock quotes. . . . we'll record your interest in technology. Then, the next time you visit,

> we might serve up an ad for a modem or an online brokerage firm or a restaurant in Akron, Ohio, depending on what we've managed to glean about you. (Boyne, 2000, p. 297).

As those strategies feed surveillance with bulky information, data subjects are not identified anymore according to their real names and habits, as expressed by the quotation. Data subjects have their identities extracted of their bodies and are seen as raw codes of numbers to large-scale bureaucracies that collect fragmented information and sort them according to their criteria. This abstraction of bodies and "souls" transform the traditional understanding of seeing and being seen, the power of the gaze. Nowadays, people cannot recognize other subjects or themselves as subjects in a traditional social position and fixed personality.

> When we recognize our name, or in Althusser's famous example, our hierarchical social position is acknowledged and produced in the response to the policeman's hail: "you there!" Without the participation of actual selves how can there be any interpellation? It would seem that with modern dataveillance, the grounded, embodied subject is increasingly left out of the story as the world is automatically made and remade around us (Simon, 2005, p. 17).

In light of the above, surveillance refers to the capacity of renaming and sorting the "self", the core information of an individual. Rather than the Foucauldian power through the gaze to discipline individuals, the Deleuzian gaze is a pure form of power with "no individuals". This power is enabled in real-time in digital flows that reinforce the need for governmentality and biopolitics, that is, the need for administrating and categorizing populations. In that sense, surveillance entails the creation of bonded physical and cognitive spaces, introducing processes designed to capture informational flows. These flows of modulation and control are like the branches of a plant spreading in many directions and like the roots that penetrate the interstices of the social substrate to expand surveillance. This vegetal metaphor was identified by Deleuze & Guattari (1988) and was denominated as the rhizomatic network. Rhizomes are plants that grow in surface extensions through interconnected vertical root systems. The rhizome is contrasted with arborescent systems which are those plants with a deep root structure and which grow along branching from the trunk. The rhizome metaphor, thus, expresses the vertical and horizontal growth of the surveillant assemblage.

In that sense, Deleuze & Guattari (1988) introduced a radical notion of multiplicity rather than the traditional approach of politics as a vertical and stable structure. The term "assemblage" describes a "multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together; they "work" together as a functional entity" (Patton, 1994, p. 158). The multiplicity of objects and methods demand a careful approach to speak about surveillance, or surveillance(s), as the interface of technology and corporeality serve different

purposes and are not concentrated in centralized watchers. The decentralization of surveillance means de-concentration and flexibility to establish "interfaces between organic and non-organic orders, between life forms and webs of information, or "between organs/body parts and entry/projection systems (e.g., keyboards, screens)" (Bogard, 1996, p. 33).

Indeed, absolute freedom does not exist, but the surveillant assemblages represent, until a certain degree, a multifaceted labyrinth of concrete and virtual tools that serve to exercise social control in many domains. If discipline traditionally emanated via institutions like the family and the army, social control now can be exercised through screens, advertisements, scripts, codes, texts, and subliminal messages. These tools deliver products and supply human necessities but they also have the potential to reproduce *The Matrix*, a discrete and unperceived monitoring assemblage that blurs the line between freedom and social control, a Kafkian dream-like reality where we do not know who observe and judge us. Because of that, it is increasingly difficult for individuals to maintain their anonymity, or to escape the monitoring of social institutions. "Efforts to evade the gaze of different systems involve an attendant trade-off in social rights and benefits". (Haggerty & Ericson, 2000, p. 619). The result is that the surveillant assemblage operates by abstracting human bodies from their territorial settings, separating them into a series of discrete flows. "These flows are then reassembled in different locations as discrete and virtual 'data doubles'. The surveillant assemblage transforms the purposes of surveillance and the hierarchies of surveillance, as well as the institution of privacy" (Haggerty & Ericson, 2000, p. 605).

The surveillant assemblage de-territorializes bodies and physical spaces adding new layers of virtual reality that return and modify the first ones. For instance, by abstracting bodies and separating them from their biological sources to create informational flows, surveillance seeks for stipulated behaviors and patterns that constitute temporal categories of suspicion and dangerousness. On security grounds, surveillance appropriates flows to turn visible which is deemed as a threat, a deviant, a criminal, and a dissident. The surveillant assemblage, in security words, can be understood as a mechanism of visualization to join the dots in case of threats and as an effort to recognize potential suspects. Surveillance, like intelligence, works in a cycle of information that enhances the "flesh/technology amalgamation comprised of pure information which is only then redirected back towards the body for a multitude of reasons" (Hier, 2003, p. 402). For this reason, the surveillant assemblage still reproduces a governmentality component of watching the abnormal to restoring normality. In that sense, dataveillance, the disassociation of body and data with its ulterior recombination for the sake of governmentality, can be deemed, in our perspective, as the extension of traditional biopolitics identified by Foucault in previous historical periods and domains.

Foucault wrote that biopolitics consists of a set of rules, a political regime, that "exerts a positive influence in life, [with] endeavors to administer, optimize and multiply it, subjecting it to precise controls and comprehensive regulations". It is a situation where power is applied to the "function of administering life" (Foucault, (1979) 2008, pp. 137-138). In that sense, biopolitics focus "on the body" and serves biological and political processes: reproduction, birth, mortality, health, life expectancy, longevity, and all the conditions that regulate them (idem, p. 139). However, when surveillance is related to biopolitics, the former cannot be delimitated to biological processes. Biopolitics is useful to understand the regulations of bodies and populations even in virtual domains. As the cyberspace overlaps with the physical reality and the former emulates the latter, informational citizens act as well as subjects for biopolitics and governmentality. In that sense, the management of personal data can be considered as well as a form of biopolitics. Personal data –unified or dispersed, attached to concrete devices or abstracted into digital flows of information- is also an object for biopolitics.

While the top-down apparatus of surveillance has been transformed into a flexible assemblage to recombine and sort bodies and data, Lyon (2002) (2006) has demonstrated that the contemporary world inclines towards classification. In that sense, surveillance is not a priori a bad mechanism for disgusting politics. But the classification and the methods to constitute flows and to sort data will determine whether surveillance purposes are either good or evil. The surveillant assemblage, thus, is a mechanism that serves to modulate normalization and exceptionality. On the one hand, it processes the subjection and the normalization through administration, social sorting, and simulation that occur independently of embodied subjects. On the other hand, it serves to classify, to profile, and to deploy exclusionary powers over individuals that are deemed as deviants and suspects. By categorizing, surveillance can redefine exceptionality through governmentality and vice versa. Surveillance last lesson, then, is that this phenomenon constitutes itself as a site of power because it mediates the transition between exceptionality and normality attached to the watched people.

Epilogue

So far, we have seen that surveillance, initially understood in a rationalist and hierarchical model can constitute a first perspective. In this one, the Orwellian "Big Brother" which assembles totalitarian and authoritarian states exemplifies the repressive logic and the top-down attempt of controlling and administering individuals by hard means. From a second perspective, the Foucaldian panoptic, as well as the Deleuzean rhizomatic surveillant assemblage, are metaphors that exemplify the array of gazes, the mobility, and the mechanisms that mold populations by hard and soft means. While the first perspective seeks to regulate private life appealing to behavioral technologies that abolish individual choices at the expanse of the watcher institutions, the second perspective is oriented to the regulation and conduction of the "self". Both perspectives are represented in the following table.

Figure 3: Two perspectives on surveillance

	Perspective I	**Perspective II**
Theoretical inspirations	Weber, Orwell	Foucault, Deleuze, and beyond
Main metaphors for surveillance	Organizations watching individuals	Panoptic and postpanoptic metaphors: one watching many; or Synoptic metaphors : many watching a few
Structure of surveillance	Hierarchical and structural, with identifiable surveilling agents	Poststructural: Surveilling agents are invisible, and surveillance is an assemblage
Means of surveillance	Repressive: production and behavioral technologies	Productive: technologies of the self

Source: adapted from Ganesh (2016, p. 176).

Some critiques might infer that surveillance, as expressed in the two perspectives, still adopts a pathological view about the gaze and consists of a governmentality simplification that classifies and excludes suspects in a friend/enemy dichotomy. This is partially true as there is a degree of simplification in both perspectives, especially when it comes to the control of subjects. But it is also important to remind that surveillance, either in the first traditional perspective or in the second poststructuralist perspective, molds individuals who in turn are not passive objects for a normalizing gaze. If the watched are sometimes "docile" subjects or data recipients, it is also true that they can behave as active subjects in the management of their own visibility. As expressed by Majid Yar:

> Such a subject enters the field of visibility empowered with various repertoires and skills of self-presentation, and cultivates a visible demeanour in line with practical projects and goals that he reflexively organises. [Moreover,] the production of a normalised moral order through mutual visual (and verbal) monitoring is the precondition not only of minimal structures of civility, but also of the co-ordination (Yar, 2003, p. 264).

Surveillance as a pre-condition of the minimal structures of civility opens the door to a relationship that escapes the mere top-down hierarchy between watchers and watched. It implies that surveillance could be also "good". Yet, surveillance does not equalize the power and political capacities of watchers and watched at the same level. In that sense, surveillance studies must alert people about the asymmetries of power between the watchers and the watched. In that effort, they must avoid simple assumptions of a subject as a malleable object, sustaining a notion of resistance that is not equal to the power that dominates it. "The increasing intensity of visual scrutiny [of the watched] does not necessarily yield a corresponding amplification in subjective self-discipline technologies of discipline" (McNay, 1994, pp. 101-102) neither of control. Therefore, if surveillance is performed to capture or regulate subjects, it opens a space in which is possible to bargain some degree of resistance. Ultimately, if subjects refuse to take the surveillance mechanisms seriously, they turn out challenging its authority and thereby threatening their disciplinary effects (Ganesh, 2016). Thus, the role that individuals play in surveillance and countersurveillance is essential and can be interpreted in two perspectives as shown in the last table. In the first structural perspective, countersurveillance is oriented toward challenging authority. In the second poststructuralist perspective, countersurveillance is understood as a mediated, contradictory, and continually reconfigured activity against sousveillance, the endless cycle of observation, or liquid surveillance (Bauman & Lyon, 2013). In short, countersurveillance is linear and has a clear ending, the victory over the surveyors in the structural or traditional hierarchical perspective. Rather, in the poststructuralist perspective, resistance is constantly exercised in multiple fronts without clear endings over an incessant and liquid surveillant assemblage. This latter is not necessarily a pessimistic view about the possibilities of resisting the evils of surveillance. Yet, this and other perspectives to resist surveillance will be worked alongside accountability and civil agency strategies extracted from the study cases in further Chapters.

To conclude, considering the theoretical discussion and the changes in surveillance, and since both of our case studies constitute transitions and consolidations of post-structural scenarios (perspective II in Figure 3), we formulate the following conceptualization for surveillance in this work:

- Surveillance is the continuous socio-technical interaction or activity addressed to collect, process, and refine information from/to certain objects with concrete or diffuse purposes. This phenomenon ranges from the mediation of power through the gaze and the self-discipline of subjects (panoptic principles), to the gaze as a site of nodal power (rhizomatic assemblage) that mediates the transition between exceptionality and normality circumscribed to the objects of surveillance (the watched). As surveillance is connected to panoptic principles and the rhizomatic assemblage, it also consists of the regulation of life cycles, development, and growth of individuals (biopolitics), and of the management of populations with the aim to constitute and sustain the dispositives that coalesce and operate the techniques to select, sort, classify, categorize and govern the heterogeneous "mass" of people (governmentality). Thus, surveillance does not equalize a relationship of power between surveyors and surveilled. It also entails a relation of power that produces different fronts of reaction and resistance to the mechanisms of governmentality.

1.3. On privacy: Basic remarks

Our subjugation is perhaps the most perverse in history
because it is voluntary and almost invisible.
Marina Garcés, 2020.

Surveillance is a phenomenon that spreads its rhizomatic tools every day in several domains. Hence, it does not require some apocalyptic vision of contemporary democracy being replaced by Orwellian dictatorships to worry about a surveillance society impacts. There are a lot of possibilities for countries to become a meaner, less open, and less righteous place without catastrophic changes –like wars and economic crises. And recent and "normal" aspects of surveillance support this vision, such as mass surveillance capacities deployed by strong states –as attested by the Snowden and Manning revelations-, the banality of security since 11/09-, and because big data corporations can become extensions of a broader surveillant assemblage. In short, exceptionality in surveillance can be fostered by everyday governmentality trends and by incremental paces.

However, we must remind that the gaze also has an inextricable link with the construction of intimate spheres and the public recognition of individuals. We exist as individuals as far as we can represent ourselves as autonomous subjects to other people. This representation is only possible as long as we can use recognized identities to protect privacy. Therefore, people need to preserve an inner space, a private sphere. It is not saying that this space is absolutely sacred and delimited. It consists in supporting the ability to transit between this space and the outside world because even the Hobbesian social contract mentioned in this chapter stipulated a differentiation between the sovereign and the subject as spaces that must be preserved.

When it comes to privacy, this idea is related to individuals' dignity and liberty. Even in ancient historic periods and in different cultures, people have struggled for the right to be respected in their physical and mental individuality. The intimate ideas and practices of one person should be circumscribed into a certain sphere where there is no interference from third parties. This space must be preserved against violence, manipulation, and deliberated subjugation of his/her autonomy as a human being. Individuals are not isolated from ideologies and political forces. Rather, it means that privacy is also related to the preservation of a certain degree of liberty, which includes the ability to contest hegemonic powers and the right to hide something for different reasons.

In the network society (Castells, 2004) almost every person wants to be seen and to see, yet also to be left alone. People value the public right to know, but also the right to control their personal information. In an overall sense, people

value freedom of expression to know and express their ideas. Yet, in ideal situations and under civic virtues, they do not want to see other individuals defamed or harassed. At the same time, the overall citizens' expectations may collide with particular interests and privacy concerns. This is true in the case of Law Enforcement, where public concerns prevail over private interests to enforce certain suspects. But the reversal can also be true: privacy can be affected by illegitimate means even by Law Enforcement. That relationship is driven by apparent trade-offs: either we choose privacy at the expense of safety, or we embrace security despite the corrosion of privacy. But this sum-zero-game is also an illusionary strategy, a direction that we are not obligated to follow. One value has its horizon related to the other one –security without privacy and individual liberty is not the security of human beings, is the protection of "slaves". Besides, the trade-off between those values is illusionary because they should be bargained to calibrate societies that guarantee privacy and dignity, instead of security societies at any cost.

Thus, a constant bargain is different from a trade-off or a zero-sum-game. Rather than solid points to defend one of these sides, "At best, we can hope to find a compass rather than a map and a moving equilibrium rather than a fixed point for decision making" (Marx G. , 2004, p. 246). Therefore, those who affirm that privacy is dead or that it does not matter do not realize that privacy is not static and fixed. Privacy, as well as other values, is bargained in tiny battles every day. At the same time, privacy should be put into the compass of meta-political goals to be pursued in a long future, even if there are no precise maps. Privacy must be there, reinforcing beautiful politics even when it seems to disappear by exceptional measures. In that sense, as exceptionality is not detached from normality, exceptional securitization that overrides privacy will result in governmentality that promotes security at any cost. Hence, even exceptional measures must incorporate privacy as a governmentality concern. Privacy cannot be simply rescued after dire exceptional measures; it matters and must be promoted *during* those measures, otherwise, the layers to reach disgusting politics will expand their thickness; avoiding the return of beautiful values such as the ability to preserve certain spaces of privacy and individual autonomy.

Those who claim that privacy is dead also mistakes this value as a wall that separates private life from the public interest. This vision claims privacy as an opaque zone or a line that protects intimate secrets. However, for the individual, privacy is not static and also serves to exercise some degree of dignity and liberty. On the internet, for example, privacy serves to control personal information and the way it is processed. The initial capacity to define how personal information is worked and the ability to verify how the representation of someone return to create individuality are very important in our age of transparency (Han, 2015), as well as in our societies of spectacle and mass culture mediated by multiple gazes (Tay, 2019). Hence, the initial capacity to govern our personal information is

crucial but not sufficient to redefine the pathological surveillance strategies that undermine privacy and increase the difference of power between subjects and data processors.

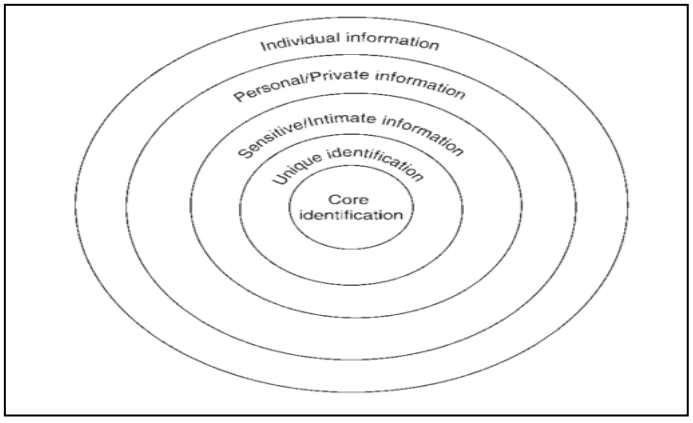
In addition, if personal information is a piece of data extracted from an individual, that piece must be considered as a strategic component of one person instead of his/her ontological image or essence. Personal information can be interpreted in philosophical terms (as the abstraction and the identification of the "being"), in technical means (such as analogical registers, digital codes, and fragmented information from a data subject), and in judicial means (for example, separating the owner and the processor of this information, and creating rights for consent and deletion of personal data). Traditionally, unique personal information served to create a core identity based on biological ancestry and family. In societies where was little geographical or social mobility, people were rooted in local networks like family, and individuals tended to be personally known. After the industrialization and urbanization of societies, core identity came related to biopolitics –the administration and power over physical bodies- that relied upon different individuals' information such as name, birth certificate, national identity, credit cards, and so on. With the expansion of biopolitics and surveillance tools, individualization tactics increased based on DNA, voice, retina, facial geometry, and other cyber/biological approximations. But even biological characteristics do not automatically represent the core identity of subjects, they constitute strategic parts to be recognized by external gazes to create a provisional identity and to validate individuality. For example, when traveling, the digitalized fingerprints and photos in a passport are checked in police records, certifying if data corresponds with specific characteristics of one person in order to validate her mobility across countries. To a person who was born and raised amidst the multitude, fragments of data and codes validate her/his individuality to the eyes of other people and authorities.

Privacy is related to personal data fragments but it is more than the mere sum of these parts. Privacy also depends on the recombination and representation of personal information. Deborah Johnson and Priscila Regan use the house of mirrors metaphor to describe personal data recombination. As when a person enters in a house of mirrors and sees his/her image distorted due to the movement and the position of the mirrors, according to those scholars, individuals information is sorted, bounced and rendered by socio-technical tools in many ways and with different purposes (campaign financing, secure flights, search engines, social networks, online advertising and so on) (Johnson & Regan, 2014). This metaphor resonates with aesthetical interventions in which visitors play with images and mirrors to see distortions and re-arrangement. Far from innocent games, those artistic interventions lead to rethink notions such as own image, personality, and identity. The cover image of this text, for instance, shows a

hexagonal mirror cannon by Olafur Eliasson with a hole in the middle in which a person's head can emerge to be reflected in all directions.

Naturally, not all types of personal information are used in the same way and have the same importance for the watchers and the watched. Therefore, scholars like Marx (2004) offers a typology to describe the kinds of personal information most commonly addressed by surveillance. This typology includes 1. Individual identification (the 'who' question). 2. Shared identification (the typification question). 3. Geographical/locational (the 'where', and beyond geography, 'how to reach' question). 4. Temporal (the 'when' question). 5. Networks and relationships (the 'who else' question). 6. Objects (the 'whose is it' question). 7. Behavioural (the 'what happened' question). 8. Beliefs, attitudes, emotions (the inner or backstage and presumed 'real' person question). 9. Measurement characterizations (the kind of person question, predict your future question). 10. Media references (yearbooks, newsletters, newspapers, TV, internet) (the minutes of fame question). According to Gary Marx, this typology of information can be represented in concentric spheres that surround the core identification of one person (See *Figure 4*). Despite he does not offer a clear conceptualization about the meaning of the "core", the inner circles are supposed to reflect more sensitive information than the external ones. The external circles (individual information and personal/private information spheres), for instance, reflect typologies such as names, family, association/affiliation, location.

Figure 4: Types of information embodied by privacy



Source: (Marx G. , 2004, p. 240)

It is thought that the more intrusive a surveillance system is, the more it can extract and alter the core identification of one person. As mentioned, in our vision, this core is more related to a strategic space/sphere where the individual constitutes her individuality rather than an ontological sphere where the individual essence is located. Even jurisdictions to control surveillance systems differentiate between private information and sensitive private information. In the case of the interception of telecommunications, the former can be exemplified by

meta-data (names, IPs, login, user number, geographic location) while the latter can be illustrated by content data (messages, voices, images attached to sensitive private spheres) collected from users. Of course, this collection is not linear and simple. It is closer to the house of mirrors metaphor in which the characteristics of information-gathering techniques and the nature of the data gathered are pieces of a broader ecology of surveillance across cultures, times, and institutional settings (Johnson & Regan, 2014).

In an historic perspective, if we transpose the two surveillance perspectives from the *Figure 3* to analyze the concentric types of personal information in *Figure 4*, it is arguable that structural surveillance (perspective I) was performed in a different fashion when compared to post-structural surveillance (perspective II) to collect personal information. While structural surveillance ensembles Orwellian nightmares as well as totalitarian and dictatorial regimes, this kind of surveillance aimed to collect and alter the deeper spheres of personal information. It deployed repressive measures to discipline the individual through behavioral technologies. It aimed to conquer and administrate the core identification by hard means. Thus, the individual needed to open his/her inner layers because he/she allegedly had nothing to hide to the gaze that ruled the sociopolitical order. Because of these intentions to override individuality to construct a sociopolitical order (especially in the case of totalitarian regimes), it is not a surprise that several forms of violation of privacy were committed by formal and informal means (like government officials watching suspects and dissidents, and informal vigilante networks that denounced "wrong" doers in neighborhoods, factories, and villages during the Franco regime in Spain). But at the same time, it is arguable that this kind of hard surveillance produced several types of resistance from individuals that enhanced counter-surveillance acts to block and avoid the power of the official gaze. Hence, despite the brutality to reach the core identification sphere, this sphere was sometimes unreachable to surveyors.

Meanwhile, post-structural surveillance (from metaphors like the panoptic and the surveillant assemblage) can reach and alter the core identification of one individual by softer means. Instead of appealing to repressive means, this kind of surveillance deploys technologies of the self; it invites the individual to produce his/her own image and to constantly create his/her core identification without direct coercion. By doing this, surveillance can reach the inner spheres of individuality insofar as individuals might offer less resistance to open the layers of their private life. This perspective of surveillance does not ignore that resistance is constantly exercised in multiple fronts. Yet, it assumes that individuals can be concerned about suspicion categories and repression but, at the same time, they can love the 'Big Brother' (McGrath, 2004) and participate in the surveillance assemblage emulating a game. Gamification means that subjectivities or users voluntarily "expose their personal information, which is then used to drive behavioral change (e.g. to weight loss, to increment workplace productivity, to

produce educational advancement, to retain consumer loyalty, etc.)" (Whitson, 2013, p. 163). The 'game' emulation of traditional social practices is used to inculcate desirable skills and behaviors. Gamification, thus, serves as an emulation of the panoptic self-supervision effect, as it provides real-time feedback about users' actions and gathers large quantities of data in the hands of surveyors. In short, in the post-structural surveillance perspective, information gathered from private spheres sustains governmentality –the dispositives for the administration of populations- reproducing the panoptic metaphor and its disciplinary effects.

While the era of structural surveillance was able to dominate hearts and minds by hard means, the digital post-structural era of surveillance is capable of reaching hearts and minds on a larger scale and with more efficiency. Because of that, the migration of a wide range of social, professional, and personal communication onto commercial platforms has raised new questions that affect privacy: what level of discloser about the collection of personal information is compatible with privacy safeguards? What types of controls should be placed on the use of personal information on a large scale? These questions are added to previous ones that were not completely answered: what levels of controls must be constructed against deviation of power? What level of tyranny is hidden in friendly and open surveillance tools if they are acceptable? Those questions are of vital importance to understand the past and the future of our societies. They matter because they help to reconstruct lessons learned from dictatorial experiences and they help to improve the accountability procedures in our political scenarios. Moreover, those questions orient the evolution and help to recognize the limits of current democracies even in scenarios without an authoritarian past.

The questions above are important to privacy, liberty, dignity, and to the life of human beings in current democracies especially because the use of software and statistics to sort populations has become a base mode of any political project and enterprise, public or private (Beer & Burrows, 2010). On the one hand, social media and surveillance have served to positive interpretations. While the migration of communication into new digital platforms still poses perils, these tools might foster interactive, participatory, mutual, voluntary, and empowerment aspects. For example, the role of social media has been analyzed in certain countries as psychological first aid tools and as a support to community resilience building (Taylor, Wells, Howell, & Raphael, 2012). On the other hand, other scholars consider social media users as an audience commodity sold to advertisers. The fact that they are content producers does not mean that media is being democratized, rather, that they are subjugated to the advent of the "total commodification of human creativity" (Fuchs, 2011, p. 288). By exploiting personal data like commodities in social platforms, this perspective enhances a certain level of alienation that reminds *The Matrix* film. In short, on the one hand, privacy and individualities are affected in positive ways, especially when the focus to analyze new surveillance platforms relies upon communication opportunities. On the

contrary, negative aspects on this matter appear when we consider infrastructure and material constraints that affect the management of personal information and the subjugation of modern "proto-slaves" that work every day to produce digital commodities for data processors.

Those interpretations are just some examples that orbit privacy and personal autonomy. Furthermore, they serve to think in solutions and political dimensions to mitigate the pathological use of personal information that produce different forms of subjugation and administrate individuals at the expense of their very individuality. In that sense, accountability might create awareness and serve as a political instrument –symbolical, institutional, rational, legal- to expose and correct the dire utilization of personal information, turning responsible those players who committed unexpected mistakes or who deliberately processed personal information without privacy guarantees. Moreover, as argued by Coleman & Jay Blumler (2009), every democratic effort should consider, among distinct principles, accountability to the public and responsiveness to public concerns, supporting the existence of a civil society sector which is free from the state and the market. Powerful surveyors -especially from state and market domains- have the ability to alter privacy in a deeper manner than other individuals and groups. Thus, accountability might replenish the relationship between data subjects and powerful data processors altering the position of the glasses in the "house of mirrors" (Johnson & Regan, 2014). In addition, accountability matters because those players sort and regulate individuals to create governmentality. As they can administrate populations by using the information related to individuals` sexuality, religion, health, death, family, personal feelings, memories, and dreams, it is time to explore the core definitions and potentials of accountability.

1.4. On accountability: The art of squaring the circle

> *I do not doubt that accountability is a problem. But exactly what sort of problem? And why so much concern about it now? Are well-understood structures for accountability failing to keep pace with real changes in how our world is organized? Or have we suddenly become sensitive to problems that were there all along? Perhaps our demands or "tastes" for accountability have shifted? […] much of the dispute about accountability is a dispute about what particular institutions are meant to do, not how accountable they are in the doing of it* (Mashaw, 2006, p. 115).

Contemporary political discourses, as attested in the last paragraph, have created a special place to the word "accountability". This word lacks from an accurate translation to the languages that represent our cases, though it is similar to the Spanish *rendición de cuentas,* and *hacerse cargo,* or to the Portuguese *prestação de contas*. In contemporary politics, a player "A" is accountable if there is another player "B" to whom the first is responsible. Accountability exists only if there is an actor who is accountable to others. Thus, accountability always has a relational aspect; responsibility on the contrary is temporally fixed and can exist without accountability. A father is responsible for their children but only when he is called to demonstrate this responsibility one can speak if he is accountable. A person can also be accountable for being a good colleague, neighbor, and citizen. In all those situations, there must be an individual or a group of people to show accountability: the actor or player "B" that holds one *to account*. In short, accountability is a relationship and a means to reach ulterior goals rather than a fixed concept or an end *per se*. As expressed in the epilogue, much of the dispute about accountability is a dispute about "what particular individuals and institutions are meant to do, not how accountable they are in the doing of it" (Mashaw, 2006, p. 115).

In this work, we will focus on public accountability, a mode of accountability *in* the public; *to* the public; and *for* the public. In that sense, not all the relational situations that imply in public responsibility are the same as accountability. Voters, politicians, and a group of citizens are audiences with different interests and relations. When those audiences are called to justify, excuse, explain, and are corrected (or when they are punished) after certain actions and motivations, accountability is on the move. If this account is given before public attention, accountability is exercised *in* the public. The account can be expressed in private rooms and behind closed doors, such as in the case of parliamentary committees that oversee intelligence services. In this case, even if the account has a restricted

audience, it aims to reach the general public. Thus, it is accountability *to* the public. Finally, accountability is *for* a certain objective and purpose.

The objectives of public accountability are multiple as this practice is delimited by scope, time, institutional designs, and resources. Yet, public accountability is primarily related to formal powers, authority, sovereignty, and duties, and rights. In the previous sections, we have expressed the importance of watching the execution of power and we have depicted some attempts to understand its nature. In the case of surveillance, the execution of power (by coercive means in a structuralism perspective or by implicit diffuse means in a post-structuralism perspective, as commented in section 1.2.), must be accountable in order to justify, explain, and correct the very authorization of authority and the consequences of its execution. In other words, **accountability not only serves to constrain power but it is also a mechanism to understand, scrutinize, negotiate, and even challenge power.**

Considering that the purpose of public accountability is an invitation to encounter the very nature of power and to redefine it, this objective can still be fuzzy and raise distinct problems. The first problem is related to whom "B" is accountable when "A" accounts for "B". This problem was called the "accountability infinite regress problem" (Dowdle, 2006, p. 39). This problem is found in hierarchical organizations and vertical chains of power. For instance, if "A" is accountable to "B", then "B" must be accountable to "C", which in turn is accountable to "D", and so on. In that sense, a new player needs to receive the account of the latter in order to avoid an unaccountable player immune to justification, explanations, and correction. By this principle, when accountability is arranged in a hierarchy, a problem emerges when the top level of the hierarchy is corrupted. Unfortunately, criminal justice, police institutions, and other security organizations might have corrupted top chief directives whose accountability does not exist or is ineffective. The solution here consists of always adding another supervisor, such as other institutions or individuals to whom the top actor of the hierarchy must be accountable.

As there are not infinite players and institutions to watch other ones, a simple solution to the infinite regress problem is to arrange the accounts in a circle. That is, if "A" is accountable to "B", then "B" is accountable to "C", and "C" is accountable to "A", implying in a circle or mutual oversight where the last player reports to the first one. "Each guardian can be a check on every other guardian" (Dowdle, 2006, p. 39). This solution to the infinite regress hierarchical problem is found in political theorists like Montesquieu ((1748) 1989). In *The Spirit of Laws,* he postulated a reciprocal system of checks and balances that inspired the institutional design of contemporary democracies. A judge must be impartial in his/her functions, and legislation must be consulted with the representatives of the people in order to be implemented. Those are cases of the republican conception of

mutual guardianship. Of course, a guardian might collude against the other one or all the guardians can turn their eyes blind to their responsibilities. Yet, the separation of powers, even by its imperfections, has shown to be more compatible with democracies than hierarchies. Before that separation, the infinite regress problem put God as the top actor to whom monarchs and divine rulers reported their accountability. Hence, the mutual checks and balances are a solution to a system where only an unreachable and divine player was able to solve the infinite regress dilemma of accountability. In that sense, it is worth remembering religious accountability as a practice that embodied asking forgiveness to God in order to absolve confessions as examples of accountable actions in some religions such as Judaism, Christianism, and Islamism. Yet, even if public leaders invoke divine entities to evaluate their actions, accountability between people, and between public institutions, is the main channel to manage politics. All religious thinking might begin with God, but it also must be worked down to man (humans). Faith and tradition are embedded in accountable actions, but accountability in the realm of politics must be checked down on Earth.

When two or more players collaborate to improve the system of checks and balances, two key aspects are still necessary: internal and external accountability. Internal accountability means that the institution "A" must deliberate with different voices and perspectives to promote the best account. The unilateral conception formulated at the top level of the organization is not sufficient to collect different accounts. In this case, this process involves dialogue and deliberation with persons from the "same" team. Notwithstanding, it is always possible to offer different judgments and justifications considering other people. Thus, on the other hand, external accountability consists of giving an account to a player positioned in a different institution with distant perspectives and motivations: the "other" team. Rhetorically speaking, internal and external accountability define the "us" and "them", the giver and the receiver of the account. But in practical terms, those aspects are still necessary. For example, in the case of restorative justice, Braithwaite (2006) has proposed that internal accountability in this field should be checked by the Rule of law. In turn, external accountability means that the Rule of law should be permeable to messages from the general public. For this author, "while deliberative accountability is cheaper and more contextually grounded […], external accountability is also needed, particularly because of the superior linkage it can offer to a rule of law enacted by democratically elected governments" (Braithwaite, 2006, p. 41). Those practices comprise the consent from the people and the capacity to make decisions based on that consent. Thus, accountability involves reshaping the understanding of authority and its legitimacy. Let us explain these concepts.

Authority is amongst the oldest and most widely used concepts in political life, coinciding with its own foundation: an Author is an originator of something, and all human artifacts as well as aggregates bear the mark of authority. Every

definition couples authority with power, but they can be dissociated in content and form. For instance, the consensus tends toward Max Weber's three-fold treatment, distinguishing tradition-based authority, rational-legal authority, and charismatic authority. Weber's "traditional authority" is a vision of tradition lodged in communities. For instance, wisdom, religion, property are rooted in a strong sense of continuity and satisfaction through loyalty that attaches members to their social positions, ranks, and superiors (Calise & Lowi, 2010). The "rational-legal authority" has permeated most functions of modern social and economic systems. It depends upon the cogency of an argument, the belief in the validity of the legal statute, and functional competence based on rationally created rules. The idea that rationality and legality ought to govern our lives has become a cultural landmark in the last two centuries. Yet, "charismatic authority" is perhaps the most controversial among the three Weberian ideal types, as it involves differences in both empirical and normative grounds (Calise & Lowi, 2010). The combination of mass politics and mass communication has made populist leadership a dominant feature in contemporary politics, as it cuts across various cultural traditions and different stages of politics and cultures.

In this study, the authority concept relates to the forms of its authorization, origins, and the capacity to deploy tools of exceptionality and normalization. From a surveillance perspective, authority does not equal power (as power is diffuse and is something that cannot be fully concentrated in one place and actor). Authority is the ability to retain, regulate, execute, and even implement social outcomes based on power and specific interactions with other players, like the watched people. A player gains authority when it has the capacity (either by tradition, rational-legal norms, or charism) to regulate the flows of power that will enhance different actions of "*imperium*" (mandates), "*potestas*" (coercion) and "*auctoritas*" (recognized prestige), either in positive ways to construct policies or in negative ways in order to block policies from other players (Calise & Lowi, 2010).

In previous sections, we mentioned the importance of the moment of origin (social contract) and the movement, from imperative and absolute mandates to the binomial tension between coercion and prestige, in order to tame and construct authority. Since authorities are not supernatural and are born amidst the will of people, the inception of authority, the authorization of authority by the people, is perhaps the most important element to be circumscribed to authority. In that sense, the horizon of expectations of authority relies on the individuals or communities that are the source of sovereignty. In other words, people authorizing authority serves as the major accountability check and balance of the socio-political order. From this level, different scales and procedures would emerge to authorize and restrain authority. Thus, to close the circle or to give meaning to authority, legitimacy appears as a complementary and interconnected value that orients authority.

Legitimacy serves power by enlarging and stabilizing its domain. It empowers commands from an authority that is obeyed by coercion or actions that are performed without the use of force. Whereas Weber defined legal-rational authority as the main form of legitimacy in complex capitalist and bureaucratic societies, there is a vast territory of legitimate power outside the direct influence of the legal system. Authority stemmed from legality and legitimacy, while highly correlated, do not necessarily coincide. The secularization of power depends upon its capacity to impose or attract (self-)interest as its legitimating force regulated through positive law. However, the law is essential but not self-validating. "Rule of law" depends upon processes by which laws are seen as by-products of successful resolution of conflicting interests. Although the Rule of law continues as a source of legitimation of control, it became only one of several sources of legitimacy, including plebiscite based on mass opinion and referenda (Calise & Lowi, 2010). The charismatic authority is perhaps the most volatile source of authority as there is a belief that the leader concentrates authority and legitimacy in the same figure. Every political leader is a charismatic authority to a certain degree (Laclau, 2008). The deviations and typologies of this form of authority are not our goals. Yet, the excessive charismatic authority must be recognized as the failed attempt to build a connection between authorization and authority, as the single party or leader reflects the attempt to simplify the whole social contract in a single person or organization. To counteract those excesses, in the last part of this study, we will address accountability principles such as consultation, participation, and presentation as forms stemmed from active citizenship to expand the territory of legitimacy.

Considering the binomial relationship between authority and legitimacy, several combinations and forms emerge to solve their tension. For instance, market and governmental players might take public decisions because they have authority, but the same decisions might lack legitimacy. On the contrary, if those decisions are taken based on representation, participation, transparency, and rule of law, it is said that those decisions "have more legitimacy because they channelize more forms and preferences from the public" (Koppell, 2010, p. 56). Indeed, an accountability process can be designed in order to be permeable to representation and participation, to enhance transparency and to protect the rule of law. These ingredients are basic steps toward public legitimacy. These steps do not define legitimacy, but their presence (even if one is absent) paves the road to a legitimated decision. At the same time, authority is not spontaneous neither is a miraculous practice. Authority to execute a decision of public interest can be taken based on real power to implement a certain decision. One organization can be legitimate before the eyes of the civil society but it can lack authority or the capacity to implement an expected decision. Sometimes authority could be deployed by exceptional and normality trends that escape to the Rule of law and a legitimate process. But either by hard or soft means, when it reaches a certain

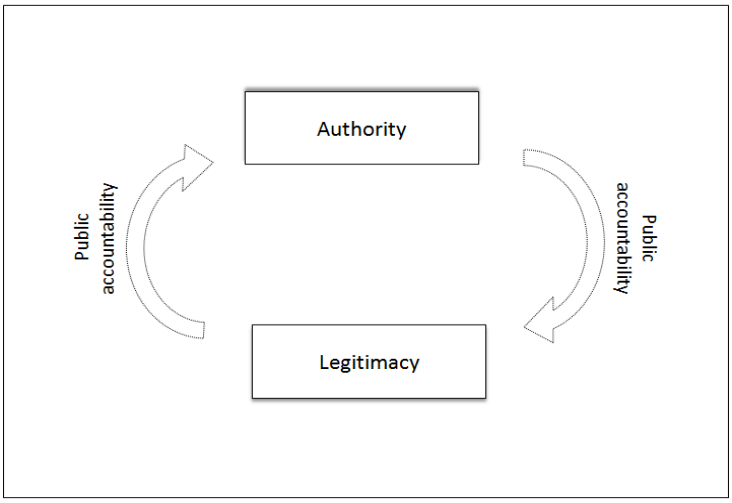
objective, authority always maintains a bargain with legitimacy. That is, authority takes decisions (normative, cognitive, symbolic, pragmatic) considering legitimacy either as a procedure or as a consequence.

In the former case, the authority to execute a decision is permeable to the steps of legitimacy during the adoption and implementation of a public decision. One example is the deliberative consultation that embodies the way in which the public budget can be spent in a city. Legitimacy here redefines the procedures that a public decision encompasses. However, in a consequential approach, authority considers legitimacy as a result rather than as a means to take and implement a public decision. A decision that affects the public can be taken without the steps that reinforce legitimacy but to improve public services or goods. For example, intelligence and national security issues are scarcely decided with direct participation and deliberation from the public during their procedural steps. But those decisions can be considered as a means to reach ulterior legitimate goals, such as guaranteeing the security of a population and preserving the public institutions of a nation. In this case, the legitimate results or consequences might justify or absolve the public decision, even if this was adopted without legitimate procedures. But a consequential perspective of legitimacy is not free of problems, for instance, decisions in security must not be unchecked during their procedures just because they have good motivations and expect good results.

So far, the legitimacy or legitimation concept in this study relates to the ground in which authority needs to build its foundation. At the same time, legitimacy functions as a teleological horizon (point of destination), a continuous mark in the compass that should be addressed by authority decisions or goals in order to avoid the mechanic rule, an empty power, and the un-fulfillment of moral and ethical bases for a public decision. Legitimacy, therefore, is not enhanced automatically by tradition or charism. In that sense, legitimacy corresponds to the authorization, the concession of authority to conduct and act on behalf of the affected parts. However, more than complying with the expectations of the majority, a leader, institution, or entity is conceived with greater legitimacy through the accomplishment of policies and actions permeated by a set of principles, such as representation, participation, transparency, rule, law, and so on that materialize legitimacy. Those principles can be incorporated in the very act of governing via procedural and consequentialist approaches, as mentioned above.

Authority can be found separated from legitimacy, and vice versa, but their tension and connection are necessary to constitute the dynamics of politics, from microphysics to structural levels of power, from small to major decisions that affect every political community, such as family, neighborhood, region, country, and humanity. Thus, the point here is to recognize that authority and legitimacy are two fronts that are always bargained during the decision and implementation of political decisions.

Figure 5: Accountability as a bargain between authority and legitimacy



Source: The author.

In light of the above, authority and legitimacy are to be connected in order to formulate and implement policies. Either by procedural steps or by a consequential approach, authority, the capacity to execute a public decision, needs to be related to a base of legitimacy. Meanwhile, legitimacy is not an auto-referential process. Legitimacy gains amplitude and scope if it is attached to an authority that accomplishes it.

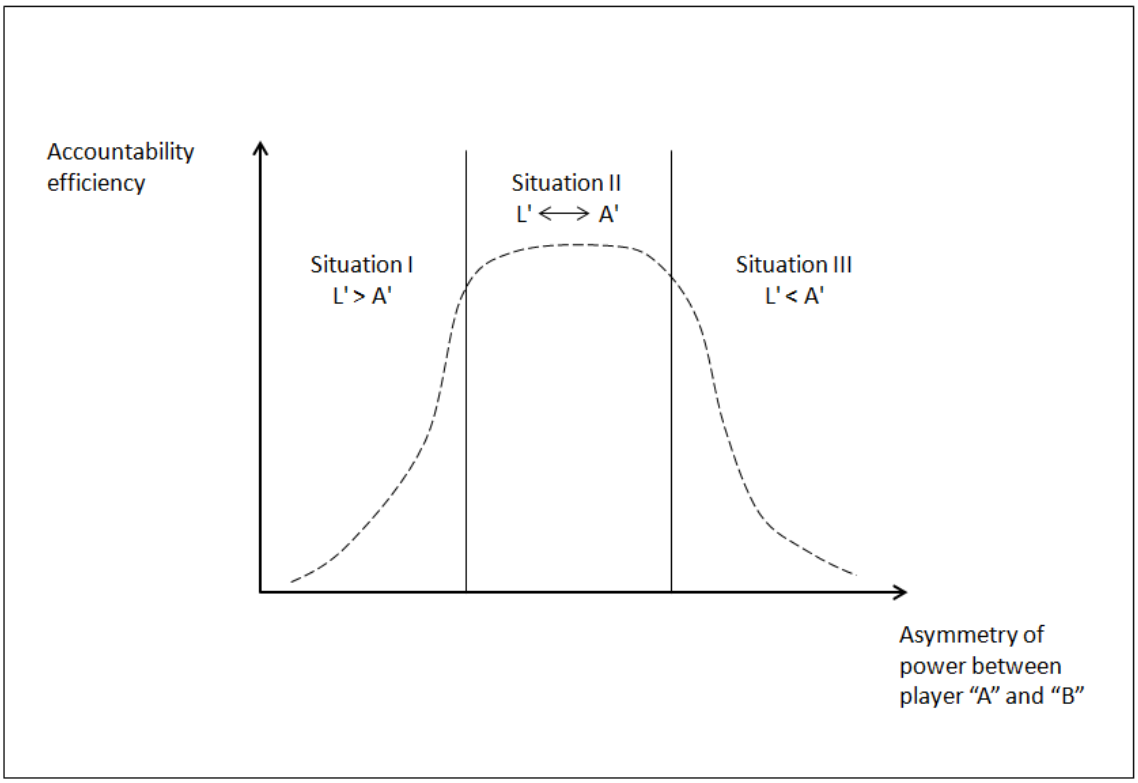
In that sense, we postulate that accountability is a connector that links authority and legitimacy. When a player "A" is called to account before a player "B", it is established a relationship that looks for a justification or a correction regarding the execution of a certain policy. In public accountability, authority is called to legitimatize their actions. But the reversal can also be true, a player can be called to account even if it has great legitimacy before the public eyes instead of authority. In this case, this player is expected to help in the execution and the delivery of policies because of its public legitimacy. A legitimate player, thus, complements and reinforces authority. The relationship between authority and legitimacy can be seen in Figure 5. As observed, accountability is activated to build a connection between authority and legitimacy. Public accountability performs as an intermediate catalyst to link both terms. In other words, accountability is a bargain, a flexible relationship that connects authority and legitimacy to the eyes of the public.

The performance of public accountability as a catalyst between authority and sovereignty is a point that also must be discussed. When authority is called to give an account, if that action does not entail more legitimacy, then accountability fails to reach its objective. That is, considering that the main goal of accountability is to put authority and legitimacy in a dialogical relationship, the efficiency of an accountability action will depend on the predisposition of both terms to establish a

dialogue. In that sense, we express three situations that will entail different types of accountability performance (see Figure 6).

Considering that accountability efficiency can be expressed in terms of the capability to establish a dialogical relationship between legitimacy (L') and authority (A'), this performance will depend on the asymmetry of power between the player "A" and "B". We call asymmetry of power between two players the difference in the capacity to retain, to regulate, to execute, or to block policies between each other. For instance, a market player, despite the lack of its formal authority, can retain more power to regulate policies than a public institution that has been created to oversee the market. In that example, there is an asymmetric difference of power between both players to adopt and implement certain decisions in that domain. The accountability efficiency, or the capacity to establish a bargain between L' and A', hence, is affected insofar as the player "B" has different capacities of power to demand an account from the player "A".

Figure 6: Accountability efficiency vs. asymmetry of power.



Source: The author.

In the situation I, there is a low asymmetry of power between "A" and "B". Both players share almost the same amount of power: the ability to retain, to regulate, to execute, or to implement a certain policy decision. In that sense, it is possible to suggest that both have similar authority. This case can be exemplified

in the accountability between individuals that share the same rank in their organizations or between institutions from the same hierarchical level in a policy sector. In that case, as there is not a sufficient difference of authority to enforce accountability results, accountability would be transformed into a dead-end road. Even if both players have great public legitimacy, as none of them has more authority to persuade, impose, or canalize accountability outputs, their legitimacy would appear disconnected from authority. This situation of grater legitimacy and poor authority (L' > A'), as mentioned before, implies that the former without the latter is an "empty" power. The low asymmetry of power is not bad per se. But even a society of "equals" must consider a player that consolidates equality by different forms of authority. In this situation, hence, the accountability bargains between L' and A' are restricted because of the reduced difference of power between "equals". For example, in local practices such as community development and participative democracy (Sintomer, 2018), citizens can enlarge the legitimacy of policies but the lack of an institutional connection or the lack of permeable authorities can undermine social innovation and the citizenship potential to deep democracy itself.

In situation II, there is an ideal asymmetry of power between "A" and "B". This means that accountability outputs (recommendations, sanctions, impositions, and other resolutions) can be adopted by the players. If "B" has greater power and authority, it can persuade or obligate "A" to modify its practices. The other way round, if "B" has less authority but retains legitimacy, it can persuade and redirect "A" to follow the accountability outputs. As there is not a dramatic difference of power between them, it is possible to suggest that accountability can be performed with sufficient efficiency because of the feasible possibilities to be transformed into a real catalyst between L' and A'. Moreover, assuming that political players tend to specialize in one of those terms and none can have the same level of legitimacy and authority, the tension between L' and A' is never solved, rather it is managed. This is because "all approaches to legitimacy set expectations that inevitably conflict with the requirements of authority" (Koppell, 2010, p. 48). On the other hand, only by deviating (at times) from the requirements of legitimacy can institutions address the contemporary problems of governance and politics. Thus, expectations to solve L' and A' in the same player and at the same time are quixotic and self-defeating. Only when there is another player that demands an account and when there is a considerable difference between L' and A', one can speak of an efficient bargain or a dialogic relationship between those values (L' ◄► A'). In this situation, the mentioned practices such as community development and participative democracy (Sintomer, 2018), can be connected with institutional channels and with administrative authorities that can enhance social innovation to deep democracy. In short, the efficiency of accountability depends on the real connection between bottom-up and top-down policies.

In situation III, there is a huge asymmetry of power between the players "A" and "B". It implies that if player "A" concentrates a greater amount of power and authority, it can execute policies without giving an account to external players. Looking for legitimacy will be only a tokenistic exercise of futility. As there is a dramatic difference in power, the player "B" would have poor capabilities to demand an account. Moreover, any attempt of efficient accountability would be short-circuited either by the reluctance of the player "A" to assume accountability outputs or by the fact that the actor "B" cannot bond or persuade the former to improve its real legitimacy. One example is when security and intelligence agencies concentrate huge amounts of discretional power, especially during authoritarian regimes. Any attempt to turn them accountable would obtain tiny results insofar those agencies can neglect information because of their last word to protect their secrets, or because the accountant has no discretional power to demand real changes from security institutions. This situation turns more dangerous as more authoritarian a certain institution becomes. Totalitarian regimes have shown that the external accountability of the "Big Brother" is an illusion insofar as they tend to concentrate power into an institutional apparatus of authority (L' < A'). Thus, one of the first measures adopted by new democracies after authoritarian regimes is to devolve discretional powers from security agencies to civilian institutions. To improve the accountability efficiency in transitional scenarios it is necessary to retire power from the military and construct institutional designs in which former powerful institutions can give accounts of their actions, like parliamentary commissions that regulate the military budget and civilian supervisors that in turn report to the elected president. Those examples are attempts to restrain the asymmetry of power between security institutions and the rest of the government, but much more has to be done to refrain the asymmetry of power before the rest of society. In short, the idea is to transform the situation III into the situation II because excessive authority, from different institutions and social domains like the military and the market, remind us that authority without legitimacy short-circuit the bargain between both values and undermines the efficiency of accountability. Finally, huge authority without legitimacy might resemble tyranny.

By the analysis of the graphic, accountability is better performed in a context of asymmetric power. But the low or excessive difference of power between the actors "A" and "B" are refractory to ideal accountability performance. Accountability is related to a situation of "quasi-equals", it is an idea that enhances democracy and democratization. That is, this value is one of the main ingredients that every democratic process must promote. Not only because it establishes a strong relationship between authority and legitimacy, but because it has the potential to be linked with other democratic procedures. For instance, as argued by Coleman & Blumler (2009), some crucial principles must be drawn as starting points in every democratic effort. Those principles are: a) regular, free and fair elections, involving competition between more than one party, b) The rule of law,

under which all citizens are subject to a common jurisdiction, c) Freedom to speak, assemble and publish, and for opposition to the government of the day to organize without fear of intimidation, d) Government accountability to the public and responsiveness to public concerns, e) The existence of a civil society sector which is free from control by either the state or the market. Although the list may continue because democracy is not fixed and comprises practices from deliberation to radical participation (Sintomer, 2018), accountability is important insofar as it can be linked with the points in the list. From elections to the rule of law and to public policies, accountability closes the cycle that connects citizens and institutions. By closing the cycle, we think in legitimizing public action and transforming authority to avoid unilateral decisions and mechanical institutional designs. Politics are not like automatic machines programmed to elect politicians, choose assets, and deliver services. Politics are permeated by inconstant roles, several players, and mutable scenarios that demand considering the public at every time, not only during the electoral process. In that sense, accountability can fulfill the promises of a stronger democracy, improving regular administrative procedures, and guiding meta-political directions (where does democracy lead us?) in the face of a mutable contingency.

As mentioned, public accountability can be transposed to improve several practices and ideas, from administration to political philosophy. However, in order to avoid a fuzzy idea that is diluted in several practices, let us reconsider accountability in its basic connotation. Accountability is a relational concept. It encompasses: (1) to whom is the accountability owed; (2) by whom is it owed; (3) for what is the person accountable; (4) what is the process by which someone is made to demonstrate accountability; and (5) what happens when she fails to meet these standards (Dowdle, 2006). These points would help to set the methodology of this work to analyze concrete policies and actions. For example, in surveillance, one can question to whom a data processor must report its account after processing personal data; who receives the account; for what the data processor was called to account; what is the process in which accountability will be shown (length, place, process, methods, legal actions, analysis, etc); and what will be the accountability output or result (recommendations, fines, sanctions, etc).

Other authors have defined similar lines to accountability. For Andreas Schedler, public accountability is a "radial" concept that encompasses answerability and enforcement. As stated by Schedler, answerability consists of the capacity and prompt response of those political players that are held to justify and legitimize their actions before others. It makes "the accountable and accounting actors engage in a public debate in the light of the public interest" (Schedler, Diamond, & Plattner, 1999, p. 15). Enforcement is a call for punishment of the accountant actor after deviations of resources, information, or power. It is understood as a stronger mechanism of accountability. Nevertheless, the "simple act of requesting information in the light of the public interest and the act of

demanding responsible justifications for decision making" are mechanisms of accountability as well (Schedler, Diamond, & Plattner, 1999, p. 17). Meanwhile, Guillermo O'Donnell gives a distinction between horizontal and vertical accountability. In short, the former is related to a relation of "equals" between institutions or individuals in a chain of power. One classic example is the checks and balances between governmental branches. The latter refers to promote accountability in a considerable asymmetric power relationship, for instance, when superior ranks account for lower officials in a hierarchical organization, and vice versa, or when the civil society ask for justifications of policymakers in the context of public decisions (O'Donnell, 1998). This author considered the asymmetry of power as the background where an account is given. Even when normal citizens demand answerability from a powerful player, accountability could exist in several forms especially when it is catalyzed by an intermediate player who can mediate the great asymmetry of power between them, like media players or courts.

Either by answerability and enforcement or by horizontal and vertical dimensions, accountability is useful to analyze surveillance. For instance, as stated by Charles Raab, in this realm, "institutions ought to be accountable to the governed, to those whose information they handle and to others who may be affected by surveillance practices" (Raab C. , 2013, p. 46). Moreover, accountability can evolve external and independent controllers as well as internal monitoring and regulators (Gray, Owen, & Adams, 1996). In addition, answerability can protect the privacy and discourage disproportional methods to sort individuals and their information. Accountability, from a functional perspective, virtually provides the reversal method of control over citizens exercised by surveillance networks (Lyon, 2007). Thus, accountability has the potential to be analyzed also in surveillance domains with different approaches. We will discuss these approaches and the objects for accountability in the methodological part.

Before that, let us consider some examples of why accountability is important in different domains. In the case of market regulation, if markets need to be accountable before the public, then several accountability mechanisms can be adopted. For example, legislative commissions might monitor privatization contracts as well as empower regulatory agencies that define certain rules, such as privacy safeguards and data rules addressed to Internet Service Providers (ISPs) and Telecom companies. Justice courts can invalidate data retention, place a stronger mechanism to oversee transnational firms, and call the executive government to clarify their decisions to reform the national economy in face of constitutional jurisprudence, especially if they detect serious erosion of public law norms or intromission into justice spheres. Moreover, internal oversight, like codes of conduct and corporate rules can spark disclosure of pertinent information, foster transparency, and of course enhance accountability. For example, corporations must disclose information and submit it to public scrutiny,

much as public agencies should do. As Andrea Headley notes, "publicly traded corporations must also submit many decisions for shareholder approval, a process that, while rarely resulting in shareholder dissent, does guarantee information disclosure" for consumers and the public (Headley & Garcia-Zamor, 2014, p. 25). Internal oversight alone does not guarantee the best forms of accountability but it is an important step that reinforces accountability efficiency. However, in the market domain, much of the skepticism about accountability is the potential of for-profit firms to serve the public interest. For example,

> If the profit motive is simply incompatible with certain policy goals, […] will private for-profit prisons actually protect public law norms? How could they, when the profit motive creates incentives to enlarge the prison population, whereas the rational criminal justice policy ought to seek to reduce it? (Dowdle, 2006, p. 96).

There is no intention to dig into this question. In the end, the balance between the public interest and the profit incentives will depend on political preferences (that are permeable to ideologies) instead of economic and rational analysis about the costs and advantages of privatization. If the economic dimension is the gun used to shot "bullet ideas" such as taxation, budget, efficiency, and efficacy, politics is the action that decides how to use that gun and pull the trigger. In the latter example, political leadership and ideology permeable to the best interest of the public and that consider the situation of the inmates certainly offers a clear inclination and automatically answers the questions arisen in the quotation.

In parallel, in electoral domains, accountability is essential to elect political leaders or parties. Here, elections serve to avoid the problem of succession and transition from a government to another one. In addition, it calls politicians to convince electors by different means. The election process must be transparent and some level of answerability and scrutiny of the past actions must exist. In that sense, regular elections can be deemed as accountability mechanisms. However, most electoral democracies present the voter with only two or three realistic choices, which means that a multitude of issues is simplified into a small decision set (Koppell, 2010). Thus, decisions taken after the electoral process must be an object of accountability. Elections are not a carte blanche for politicians. The fact that a leader or a party has been chosen to represent a group of citizens does not allow them automatically to speak in the name of those people, neither is it a form of accountability. Representation and consensus are created continuously. This continuous task might be a burden for politicians that use to speak with single voices or advocacy groups. But when a government takes a decision, for example, in the name of security, this decision must be accountable before/after it has been taken.

Accountability cannot be used to describe the mere official discourse to voters, or the devolution of authority from the central government to local institutions. As mentioned, accountability increases insofar as there are more chances of one player to demand explanation, justifications, and impose corrections to the other one. But no institution serves only one purpose or goal, and, therefore, no institution should be expected to be responsive to only one form of accountability regime. One single actor might give multiple accounts to several players and at different times. Accountability is related to repetition and is a temporal sequence instead of an isolated practice. Thus, accountability can be studied from a historical perspective.

However, some problems can be identified when accountability is performed several times during a certain period: First, accountability can become a symbolic practice that loses real efficiency. Second, accountability might turn into a witch-hunting campaign instead of promoting civic values. Third, accountability might be confused with transparency and vice versa.

In the first problem, the repetition of accountability can transform it into a simple protocol, which is valued according to its procedures rather than to substantial outputs and results. It was said that accountability is a relational concept, but in some cases, it can be misunderstood as a final goal. When accountability is performed in regular procedures or protocols, Gunther Teubner has argued that many institutions face what he called the "regulatory trilemma". In Teubner, institutions need to be simultaneously coherent (to the rule of law or regulatory norm), effective (to accomplish the norm), and responsive (which means that they must be opened to the influence of social demands and cultural changes) (Roth-Isigkeit, 2018). The trilemma for Teubner is that virtually any attempt to reinforce one of these demands works to limit the capacity of the regulatory institution to satisfy another. It is difficult, if not impossible, to accomplish satisfactorily the three points in the triangle. In this case, accountability can become a tokenistic exercise if one institution chooses to reinforce only one part of the triangle or when it fails to perform at least two parts.

In the second accountability problem, political polarization between accountants and accounters are expected, but when they trench their positions, accountability practices could be transformed into a tribunal that seeks to hunt witches everywhere. If there is a simple motivation to punish or defeat political adversaries, accountability can be performed in a culture of suspicion and accusation. A culture in which people explain themselves either with fear or intending to make a favor to the eyes of supervisors and correctors. Moreover, excessive concern to bring efficiency to accountability can produce backfire effects. For example, when accountants demand to justify every political procedure, "every penny spent" for the sake of economics and administrative efficiency, the result can be misleading. In the "New Public Management" paradigm, the system of

accountability on which public officials have to demonstrate and justify extensively many bureaucratic procedures turns out paralyzing what was supposed to be a flexible and efficient policy. Public institutions need to offer services by producing larger amounts of information and following several rules, but an environment of excessive demand for "efficiency" and distrust reinforces an idea of total inefficiency and suspicion. The more this logic comes to be taken for granted to run public management and everything else, the more suspicious everyone is. "People must be up to do something, […] because the system constantly accuses them of being up to something" (Dowdle, 2006, p. 242). As a consequence, when distrust reigns and people are implicitly accused of wrong-doing, they become less motivated to cooperate in the activity in respect of which they are accused. Possibly they become more inclined to mask wrong-doing and react defensively for fear of what will become if they reveal their mistakes. In short, tons of accountability in a culture of excessive efficiency and suspicion undermine virtuous ideas that tolerate political mistakes and serve to correct institutions. Finally, considering that accountability evolves deliberation, in this culture, people are not encouraged to explain themselves honestly for fear that every little deviation will cause punishment.

The third accountability problem happens when this is mistaken with transparency. As mentioned above, accountability is a relation that aims to connect authority with legitimacy. In turn, legitimacy can involve representation, participation, transparency, and rule of law. In that sense, transparency is just one part of the equation that explains public accountability. It is plausible that certain accountability actions, like intelligence commissions, are performed without great levels of transparency due to national security safeguards. But a reduced level of transparency should not be a death-end road. Low transparency must not be a barrier to accountability performance insofar as there are other concepts and parts of the equation that can be mobilized to improve this action. From the perspective of intelligence and security agencies, one accountability attempt must not be confused with the transparency demand to snoop around official secrets. There are ways to turn secret issues accountable by distinct methods, but again, the prerogative of *arcana imperii* does not excuse someone of hiding and classifying information with total discretion. Total opaqueness is an extreme position that must be avoided as well to protect even the most important secrets and issues. On the other hand, total transparency is an illusion that embodies perils. As freedom of information, as a requirement in political management, in business administration, in the regulation of markets, or in social responsibility guidelines, transparency is the key to the good functioning of all these human initiatives. The problem is that while stronger political groups work to mask actions and keep official secrets, there is an uninterrupted interconnected exhibition in the side of the weaker groups –the normal citizens. This "total transparency" that unveils one side leads to a sort of compulsory loss of freedom and greater control in the

surveillant assemblage. This problem is explained by Byung-Chul Han in the *Society of Transparence*. For Han, the ultimate cause of total transparency is anthropological: more and more transparency enhances distrust, which in turn enhances greater vigilance imposed to cover the offer and the demand for transparency. According to him, the society of control has a subject that appears in total transparency, not by external coercion, but by the need engendered in herself (the "normal" individual) to renounce private and intimate spheres in order to exhibit oneself without shame (Han, 2015). Total transparency endangers trust insofar as this value depends on not knowing the completeness of other persons, on some layers of opaqueness; trust means to build a positive relationship with other ones that are not totally transparent. When total transparency dominates, there is no room for trust. "The society of transparency is a society of mistrust and suspicion" (Han, 2015, pp. 91-92). To Han, as confidence disappears, individuals start to live in a society of social control and lose liberty.

Considering the problems of accountability, it is essential to express that public accountability, on the other hand, is a modest concept. As stated by Schedler (1999), accountability only is performed as a relational concept, rather than a substitutive action. That is, accountability seeks to establish a connection between two or more players, aiming different results over those players. Traditionally, accountability does not seek to abolish one player or radically transform the relationship between them. When an intelligence commission demands an account from intelligence services, the former does not seek to replenish or abolish the whole intelligence policy, at least not in the short term. Accountability nature is reformative instead of disruptive. However, it does not mean that accountability can redefine institutional designs and deeply constrain powers in the long term. The virtue of accountability resides in its modest and auxiliary nature. By restraining power, accountability reshapes power and bargain the forms to its distribution, execution, or implementation. We must be skeptical about accountability promises and outputs. Yet, accountability must not be regarded as a mere appendage to transform politics. Learning from failures in accountability experiences should be of importance for every political project that leads with legitimacy and authority. Even radical aspirations and revolutionary projects must put more attention into this practice as past attempts had shown that radical changes also failed to bring legitimacy and accountability after revolutions. After exceptional measures to transform politics, governmentality measures failed to deploy a connection between the governmental apparatus and the people. In the name of a better future, authority appeared disconnected from legitimacy as a constant process that needs to be implemented and demonstrated every day. In those cases, authority understood legitimacy as an automatic consequence that justified the centralization of power and the control/vigilance of almost everybody. For example, distant from Rose Luxemburg affirmation that Marxism should have consisted of a "continuous experience", the *experimentum mundi*, with a common

commitment to construct socialism; socialist regimes became rigid bureaucracies with political police forces and excessive power concentrated in parties with “one thousand eyes”. Unfortunately, current trends attached to western liberal politics can also reach the same destination: authority disconnected from legitimacy, controversial securitization, and surveillance that might be ubiquitous and pathological. Thus, it is difficult to imagine and dream about better futures (even if meta-narratives seem to have collapsed) if there is no place for the principles of accountability in the politics of tomorrow.

Finally, if efficient and good accountability actions belong to the realm of beautiful politics, as expressed in the first section, it implies in never giving up on responsibility, transparency, answerability, and enforcement as dimensions attached to politics. Accountability is an exhaustive practice of turning someone accountable, it is the means, not the ending goal to redefine and alter politics. In the first section, we have also mentioned that accountability consists of a relationship of controlling the uncontrollable. Hence, accountability strength stems from its initial modest promises; it can serve as the achievement of unreachable dreams by incremental paths, or to be more realistic, it can avoid reachable nightmares by redefining everyday-tiny political practices.

Epilogue

This section mentioned that accountability is a relational principle that consists of demanding accounts from a certain actor, such as justification, explanation, and even establishing a sanction. It entails a modal relationship between two or more actors that communicate by internal or external accounts insofar as they maintain social and political bonds that range from reciprocity, interdependence, to dissonance and conflict. Accountability efficiency depends on the predisposition of the actors to establish a nexus, and its ideal conditions occur in situations of intermediate asymmetry of power. We mentioned that the circle of guardians and mutual checks and balances are solutions to the infinitesimal regressive problem of accountability. And, as social actors are situated in different social positions, we mentioned radial directions of accountability, such as internal, external, horizontal, vertical, and third dimension (international). In addition to those organizational directions, answerability and enforcement are lines that explain the capacity to demand answers/justification or to impose sanctions on other actors, respectively. At the same time, we mention that accountability is a modest concept and sometimes it can deviate into tokenistic practices with no real efficiency, witch hunting campaigns that override civic values, and practices that mistake forms to promote transparency. All the same, accountability is the glue or sticky material that re-arranges social positions between social actors, thus, its

liquid and flexible nature can be used to analyze other modal activities such as surveillance.

In this study, accountability is relational and has many faces, but it follows concrete modus operandi. In this action, it is essential to know: (1) to whom is the accountability owed; (2) by whom is it owed; (3) for what is the person accountable; (4) what is the process by which someone is made to demonstrate accountability; and (5) what happens when she fails to meet these standards.

The modus operandi, in turn, has a major objective that hinges around our accountability conceptualization. In this study, the accountability concept consists of the activity conducted between two or more social actors, by informal or formal terms, in order to bargain or potentially reallocate authority and legitimacy. The reallocation can be conducted in short-term outcomes that affect the initial actors, or in unforeseen and long-term consequences that affect third actors. In short terms, accountability is the connector or the dialogical tension that links authority (object) to replenish/create legitimacy (objective) before a certain audience. Here, authority relates to the forms and capacity to deploy tools of exceptionality and normalization. A player gains authority when it has the capacity (either by tradition, rational-legal norms, or charism) to regulate the flows of power that will enhance different actions of "imperium" (mandates), "potestas" (coercion) and "auctoritas" (recognized prestige), either in positive ways to construct policies or in negative ways to block policies from other actors. In turn, legitimacy here is not enhanced automatically by tradition or charism. Legitimacy corresponds with the authorization, the concession of authority in order to conduct and act on behalf of the parts. However, more than complying with the expectations of the majority, a leader, institution, or entity is conceived with greater legitimacy through the accomplishment of policies and actions permeated by a set of principles.

In this study, as discussed in the previous pages, the set of principles attached to legitimacy are responsibility, transparency, answerability, and enforcement. The list of principles is not hermetic and can be added with other ones. Yet, responsibility relates to the basic content and functions that are supposed to be fulfilled by a certain authority. It refers to duties and missions owed or expected by one player (authority) to the accounter or/and to a certain audience. It allows identifying the actors and the content of the accountable action. Meanwhile, transparency represents a channel in which the accounts can be demonstrated to a certain audience and/or to the general citizenship. It refers to the degree of visibility, exposition, and openness. During the process of accountability, transparency allows the verification of its range and scope (actors, audiences, processes, content, time, and outcomes). Responsibility and transparency help to operationalize (1) to whom is the accountability owed; (2) by whom is it owed; and (3) and for what is the person accountable. In turn, answerability and enforcement are related to the capacity to demand answers/justification or to impose punishment on other actors, respectively.

Answerability is the capacity to demand "answers" and formulate corrections to the accountable actor(s) by soft means. It relates to trust and checks and balances. Enforcement, in turn, is the capacity do demand "answers" and impose corrections to the accountable actor(s) by hard means. It relates to the "Rule of law". Both answerability and enforcement help to answer (4) what is the process by which someone is made to demonstrate accountability; and (5) what happens when she fails to meet these standards.

In light of the above, the more those principles are encompassed in one account, the more accountable is a certain action. This set of principles allow to assess the "quality" of accountability insofar as the more one can verify their existence in a certain account in terms of discourses and concrete actions, the more there is potential to reallocate authority towards the expansion of legitimacy, which is the ulterior objective of accountability. For example, if responsibility is the product of a certain account action (such as reports released to the press in order to show the duties of one organization that upholds authority in a certain issue), this means that accountability is in the move. Yet, if the accounts involve transparency in that same process, as well as active forms of releasing information to assess policies and previous outcomes, then, greater levels of accountability are supposed to be reached. Moreover, after the wrongdoings of that organization, if an external actor is able to "extract" not only responsibility and transparency, but also justifications, explanations, and promises of modification in the initial behavior of the initial actor, then one can speak of greater levels of accountability. Finally, if the internal/external actor is able to achieve the previous principles plus the correction of the accountable organization through mechanisms of Rule of law, like sanctions and court decisions, then accountability reaches greater levels of quality and scope. It does not mean that every accountability action should comprise all the set of principles and needs to result in sanctions or punishment after wrongdoing. Accountability objective is to replenish the legitimacy from a certain potestas/auctoritas attached to one person or entity. Most of the accountability actions might work only with few of those principles reflecting their modest nature. Moreover, legitimacy can be replenished through incremental pace and by soft-power means. Thus, the interconnection between different accountability mechanisms would imply adding forces and illuminating blind spots not reached by specific forms of accountability. In that sense, we will address a mosaic of accountability mechanisms in surveillance considering two case studies: the Spanish and Brazilian surveillance assemblages in the last decades. In the next chapter, we will expose the methodology and operationalization of accountability in both cases. Now we summarize the main theories and concepts that were analyzed so far in order to operationalize this study.

Table 1: Main theoretical concepts in a glimpse

Beautiful and disgusting politics: As politics relate also to presence, emotions, and feelings, not only as aesthetical forms of apprehension but also as layers that affect and sustain social transformations, beauty, and disgust in this study are forms to equalize "good" and "evil". This simplification is not far from problems. Yet, beauty and disgust dialogical relationship helps to understand that beautiful and disgusting politics are not symmetrical opposite sides of the same coin. The former has a limited potential to penetrate the layers of the latter, whereas the latter can be reproduced without mediation and no fully understanding from a certain audience. Beauty and disgust are not equal to morals and ethics (correct and incorrect actions). Yet, they cut across those dimensions and help to recognize the importance of creating "beautiful politics" (such as mutual care relationships between people, assertive legislation that promotes justice, accountability attempts to counteract violence and corruption) despite their limited range to tame evil or disgusting actions. The continuous tension between beautiful and disgusting politics shows the importance of controlling the uncontrollable (I).
Exceptionality: The ability to create "new" politics. In other words, it is the generative dimension of power. It refers to the foundational moment or to the deep alteration of the conditions that allow the exercise of authority, its procedures, and mandates. In a Schmiddtian perspective, it refers to the capacity to decree the state of exception or to define the "us" and "them", "friends" and "foes", "beauty" and "disgust" in a certain sociopolitical order. **Governmentality:** The ability to sustain politics. It is the generating dimension of power. It refers to the iterability (imperfect repetition) of mandates and dispositives stemmed from a certain form of authority that points out to the foundational moment of exceptionality, in order to reproduce and replicate authority every day. From a Foucauldian perspective, it refers to the reason for government: the array of dispositives to regulate, categorize and govern a population distributing ab-normality and those who are targets of intervention to the eyes of authority. Both the generative and the generating dimensions of power are not disconnected in the exercise of every form of authority, from the coup-de-état to the reason-de-état, or from high politics (like national security and the declaration of war) to the microphysics of power (like everyday decisions and mundane use of data). Thus, **exceptional-normalization** indicates a process that promotes governmentality with a greater scale of exceptional measures. On the other hand, **normal-exceptionalism** indicates a process that hinges on governmentality but still is potentially connected to exceptional measures. Setting a wall to separate exceptionality and governmentality in politics would constitute an aporia: a dead-end road or a problem with no solution. This has a consequence to utilitarian approaches to politics, as means cannot be fully separated from endings (neither in temporal or spatial dimensions), and to accountability, as every form to restrain authority would be insufficient and incomplete due to the exceptional features of power. The tension between exceptionality and governmentality (normality) also helps to demonstrate that accountability and every attempt to tame power from authority are forms of controlling the uncontrollable (II).

Surveillance concept:
Continuous socio-technical interaction or activity addressed to collect, process, and refine information from/to certain objects with concrete or diffuse purposes. This phenomenon ranges from the mediation of power through the "gaze" and the self-discipline of subjects (panoptic principles), to the gaze as a site of nodal power (rhizomatic assemblage) that operates the transition between exceptionality and normality dimensions circumscribed to the objects of surveillance (the watched). As surveillance is connected to panoptic principles and the rhizomatic assemblage, it also consists of the regulation of life cycles, development, and growth of individuals (biopolitics), and of the management of populations to constitute and sustain the dispositives that coalesce and operate the techniques to select, sort, classify, categorize and govern the heterogeneous "mass" of people (governmentality). Thus, surveillance does not equalize a relationship of power between surveyors and surveilled. It also entails a relation of power that produces different fronts of reaction and resistance to the mechanisms of governmentality.

Accountability concept:
Activity conducted between two or more social actors, by informal or formal terms, in order to bargain or potentially reallocate authority and legitimacy. The reallocation can be conducted in short-term outcomes that affect the initial actors, or in unforeseen and long-term consequences that affect those and third actors. In short, accountability is the connector or the dialogical tension that links authority (object) to replenish/create legitimacy (objective) before a certain audience.

Accountability modus operandi:
(1) to whom is the accountability owed;
(2) by whom is it owed;
(3) for what is the person accountable;
(4) what is the process by which someone is made to demonstrate accountability; (5) what happens when she fails to meet these standards.

Accountability principles to assess its quality:

- Responsibility: Duties and missions owed or expected by one player (authority) to the accounter or/and to a certain audience by formal and informal means. It allows identifying the actors and the content of the accountable action.
- Transparency: the degree of visibility, exposition, and openness. During the process of accountability, transparency allows the verification of its range and scope (actors, audiences, processes, content, time, and outcomes).
- Answerability: The capacity to demand "answers" and formulate corrections to an accountable actor(s) by soft means. It relates to restoring trust and mutual oversight, including checks and balances.
- Enforcement: The capacity to demand "answers" and impose corrections to an accountable actor(s) by hard means. It relates to the "Rule of law" and justice to guarantee individual rights.

Legitimacy consists of the normative conditions emanated from the will of the people (i.e. the governed) that is expanded and improved by the presence and convergence of the above principles. More legitimacy implies that a certain action promotes those principles or facilitate the convergence of most of them. Example: a certain policy is more legitimate if it promotes or is permeable to responsibility, transparency, answerability, and enforcement in a systematic and continuous manner.

Chapter 2. Methodology and Operationalization

Surveillance comprises several activities and is executed through exceptional and governmental mechanisms. But one of the main ideas of surveillance is related to the capability to watch and regulate individuals in order to shape power and create the conditions for the comprehension of social reality. In part, we see the world as it is because people surveille other people as well as the world where they live. Surveillance could have a connotation of secrecy and violence but it also can be executed with the consent of their targets, with no direct coercion, and can serve to manage individuals and entire populations.

This latter idea links surveillance with the idea of biopolitics. Biopolitics is based on biopower, a dimension of power exercised traditionally over physical bodies. Since the industrialization of western societies, Foucault wrote that biopolitics consists of a set of rules, a political regime, that "exerts a positive influence in life, [with] endeavors to administer, optimize and multiply it, subjecting it to precise controls and comprehensive regulations" (Foucault (1979) 2008, p. 137). In that sense, biopolitics focus "on the body" and serves biological and political processes: reproduction, birth, mortality, health, life expectancy, longevity, and all the conditions that regulate them (idem. p. 139). Since this interpretation, other scholars have worked life outcomes from power.

In turn, Agamben (1998) refers to biopolitics as the inclusion of human life in the calculations of power (1998); while Lobo-Guerrero (2007) expresses the concept as "power over life". Besides, Esposito (2013) affirms that biopolitics is made by a process of immunology through which a population is protected but also confronted with the phenomena that might cause its death. However, this exposure is made in controlled levels as in the process of creating immunologic responses against diseases. The confinement of populations during the last global pandemics in one clear example of this kind of biopolitics. Indeed, recent trends on mass surveillance as well as the forms to manage critical events, such as pandemic diseases in some countries in the last times, reinforce the idea that the whole population can be a target of surveillance.

More than a disciplinary mechanism, biopolitics acts as a control apparatus exerted over a population as a whole. When surveillance is related to biopolitics, it refers not only to mere administrative tools and tactics to collect information; but also to conduct a social experience in a certain place where all individuals are goals and means to the deployment of a diffused power. Besides, biopolitics starts but is not delimitated to biological processes. This concept is useful to understand the

regulations of bodies and populations even in virtual domains. As the cyberspace overlaps with the physical reality and the former emulates the latter, informational citizens act as well as subjects for biopolitics and governmentality. In that sense, the management of personal data can be considered a form of biopolitics. Personal data –unified or dispersed, attached to concrete devices or abstracted into digital flows of information- is also an object for biopolitics.

Now, considering that surveillance is related to biopolitics, it is important to notice that the administration and regulation of populations are conducted either by "good" or "bad" motivations. Surveillance is important to bureaucracies, services, communication, and helps us to live in society. Social welfare, education, and other domains gather and process information from individuals to improve services and policies. Not all forms of surveillance are pernicious and evil. Since we are social animals, we share our data and present ourselves before other people for different reasons. But as expressed in the theoretical discussion, surveillance is not about the gaze per se (the representation of ourselves and other people), but is related to the manners in which the gaze is constructed, used and transformed. Thus, admitting that surveillance is a vital component for contemporary politics, it is possible to express that this phenomenon also presents a negative side: a pathological dimension attached to its array of practices.

Pathological surveillance consists of the use of the "gaze" and of biopolitics to regulate populations according to principles that are ethically, cognitively, and aesthetically wrong in the sense that they can abolish individuality to regulate people. A proof of pathological surveillance can be exemplified with the commodification and the disproportional surveillance of personal data. The commodification of personal data consists of the acceleration of the commercial architecture of participation on the Web that stresses "exploitation and enclosure, transforming users into commodities that can be sold on the market" (Petersen, 2008, p. 7). A complete definition of the commodification of personal data and the alienation of users is defined by Mark Andrejevic in these terms:

> These commodities [user data] are distinct from the Tweets, posts, uploaded videos, and so on, and yet they are the result of user activity. They are commodities with market value and while they are created by users, they are not controlled by users, who have little choice over how and when this data is generated and little say in how it is used. In this sense we might describe the generation and use of this data as the alienated or estranged dimension of their activity. To the extent that this information can be used to predict and influence user behaviour, it is an activity that returns to users in an unrecognizable form (Andrejevic, 2011, p. 286).

Christian Fuchs goes further in the idea of the commodification of personal data expressing that the contemporary Internet is a specific platform based on the exploitation of "prosumers" (producers and consumers) that create data. This

argument could be summarized as the realization of digital techniques through which prosumers are electronically sorted and exploited. They create content and information that return to them in vicious forms, in the form of commodities. Therefore, "the category of the prosumer commodity does not signify a democratization of the media towards a participatory or democratic system but rather the total commodification of human creativity" (Fuchs, 2011, p. 301).

As expressed above, advertising and monitoring people are not bad practices a priori, but they can be worked to produce docile subjects which in turn are targets for consumer alienation, as expressed by Fuchs, paving the road to intrusive and unaccountable surveillance. For instance, when personal data is commodified or serves for unclear security purposes, digital flows constitutes power and feeds a disciplinary surveillance assemblage that identifies, classifies, and assesses individuals (Gandy Jr, 2012). Prosumer commodification on Web 2.0 identifies the interests of users by closely surveilling their data and personal behavior. In that sense, some authors such as McGrath (2004) and Whitson (2013) mention that the power of surveillance could attract or seduce their targets either in terms of loving the "Big Brother" (the watchers) or in terms of gamification. Gamification means that subjectivities or users voluntarily "expose their personal information, which is then used to drive behavioral change. It serves as an emulation of the Panopticon self-supervision, as it provides real-time feedback about users' actions and gathers large quantities of data in the hands of surveyors. In short, those examples constitute clear cases for governmentality and biopolitics but they are not neutral. They can also foster the pathological surveillance of subjects. In that sense, not only personal information is a valuable source for commercial advertising, but it also sustains the surveillance assemblage, reproducing the panoptic metaphor and its disciplinary effects.

By the previous theoretical discussion on exceptionalism, governmentality, and privacy, it is not possible to assure where are the limits between "good" and "pathological" surveillance. It is impossible to build a dam to isolate the good motivations to administrate populations from the misuse of privacy and from bedevils behind that same administration. Because of that aporia, accountability was expressed as a continuous practice that might be performed to redefine surveillance and counteract its pathological side. The relationship between surveillance and accountability constitute, thus, our hypothesis.

2.1. Hypothesis

Surveillance has different purposes, but here it must be understood as an especial component for the administration of populations through the deployment of exceptional and governmentality measures (see surveillance concept in section 1.3). Therefore, considering that surveillance is related to biopolitics, the administration and regulation of physical bodies and populations by the extraction and analysis of individuals information in a certain place and time, there could be some strategies to mitigate or redefine the disgusting or pathological side of surveillance (un-checked, disproportional, intrusive, inconsequent and banal use of surveillance) that abolish the autonomy of individuals and increases the power distance between watchers and watched. Those strategies, in turn, can be reformulated into this: Provided that some political players are responsible for the management of individuals' information, we want to assess and verify whether accountability could mitigate or radically transform "disgusting politics" of surveillance.

Therefore, the overall objective of this work is to analyze and assess accountability mechanisms that were deployed upon surveillance practices in specific places and domains. Those places are Spain and Brazil since 1975 to 2020. We consider intelligence agencies and personal data as objects or domains for this study. We will explain the spatiotemporal division and the selection of those objects in the operationalization.

Considering the hypothesis, as secondary objectives, it is important to verify how accountability can redefine surveillance in terms of:

- The management of information to preserve subjects' autonomy in a specific population
- The asymmetries of power between those who watch and those who are watched

By subjects' autonomy, we refer to some level of privacy and auto-representation that individuals adopt in the face of surveyors and within the surveillance assemblage. It is the capacity to act as an individual, a sovereign person, in surveillance contexts that can erode not only privacy but also individuality. Autonomy related to privacy is essential insofar as the lack of this characteristic overrides any understanding of active citizenship and individuality to construct social ties. Besides, subject autonomy could be related to civil and political rights that are the normative foundations of contemporary sociopolitical orders that refer to themselves as democracies. On the one hand, those rights are normative conditions that inspire democracies; on the other hand, they are shaped, transformed, and adapted in surveillance either by exceptionality or governmentality measures. Thus, the normative dimensions of individual

autonomy stem rights that surveillance practices are supposed to consider such as integrity, proportionality, responsibility, and other fundamental civil and political rights. In that sense, subjects' autonomy and individuals rights must be understood as normative metonymies to be extended or preserved to the whole sociopolitical order, to the overall population in a democratic regime, instead of being restricted to privileged and powerful individuals or to none. We used the word metonymies because those rights overlap and are a pre-condition that enhance but do not summarize individual autonomy. Individual autonomy can also be understood as the core object behind the brief epistemological history of power and sovereignty (see Chapter 1). It represents that individuals are components of the people that authorize authority and stem legitimacy. Yet, they simultaneously distinguish and interdepend on collectivity. At the same time, collectivities are not the mere sum of individuals and present differences of power that constrain normative opportunities, material conditions, and even ideas of liberty and justice. Every social order has differences of power that affect collectivity and individuals. Some of them are so exponential that disable individual autonomy and cut across specific issues like income, gender, race, nationality, education, labor, accessibility, age, language, etc. These issues are factors that influence power asymmetry and even redefine surveillance as a domain in which watchers oversee watched people. Thus, in this study, surveillance is also connected with those factors as not all the watched individuals are treated in the same form or receive the same impacts.

By asymmetries of power between those who watch and those who are watched in surveillance, we mean a difference of power that implies a dynamic relationship between authority and legitimacy as explained in Figures 5 and 6 in the previous Chapter. In that sense, this study wants to verify what kind of asymmetries of power exists between certain watchers and watched and how accountability can replenish the dialectics between authority and legitimacy. For example, a huge power difference between watchers and watchers is refractory to accountability efficiency. This situation represents a point that compromises the link between authority and legitimacy and could enhance different forms of deviation of power, including direct tyranny and tacit hegemony. A situation in which there is low asymmetric power between watchers and watched is also refractory to accountability efficiency (Situation 1 in Figure 6) but is not the focus of this work. Since we focus on macro-social and public surveillance at the level of nations/states, the best form to analyze accountability is to assess surveillance mechanisms that have the potential to affect large groups of people and handle considerable quantities of information. This simulates a situation of strong (situation 2) or huge (situation 3) asymmetric power that demands more analysis. Surveillance in contexts such as family, workplace, neighborhood, and other micro-social domains are not direct targets of our effort as they constitute situations of lower asymmetric power at the structural level or at the scale of nations and states. Surveillance in public spheres that affect large populations such as

education and economic policies are also outside of our range. Instead, our objects are intelligence institutions and personal data networks.

The first reason for that selection is explained by the fact that surveillance is the main activity that guides politics in those domains. Intelligence is a traditional form of state surveillance that enhances biopolitics. Traditionally, it was a social domain related to exceptionalism in politics. Personal data, in turn, is a crucial object that feeds the surveillant assemblage with bulky amounts of information and power. Therefore, personal data is crucial governmentality dispositive in the hands of surveyors. The second reason is that those objects historically have been outside of the scope of civilian oversight and accountability assessment. In that sense, by choosing those objects, we aim to contribute to analyze practices that are usually understood as distant for most of the 'common' citizens, either by political secrecy or by technical opacity. Because of the secrecy, technical expertise, restricted access, and because one of those objects is associated with the "black box" of political regimes, this work reconstructs the meanings of those objects and sheds light upon them by using a specific operationalization.

2.2. Operationalization

In a first approach, one can consider accountability as the independent variable to be analyzed alongside surveillance (dependent variable) because it is believed that the former can redefine the latter. Yet, it is difficult to think in strict causal relationships between both dimensions. Firstly, accountability and surveillance are multi-relational flows; they cannot be simply juxtaposed or contrasted to verify precise correlations even if they exist sometimes. Accountability is as flexible and malleable as surveillance and their relationship can be programmatic but also contingent. Secondly, since we cover different domains and heterogeneous practices in societies, the diversity of social relations resembles complexity models and multidimensional dependences rather than linear causation between two variables. Thus, we divide the study in two realms using multiple tools. In the first realm, we follow social sciences and historical analysis, such as constraint legacies, path dependence, and critical junctures patterns to analyze intelligence and accountability interdependences. Whereas, in the second realm of personal data, the proliferation of new technological and social domains demands a holistic approach such as policy network and governance analysis.

Considering that, we focus on two cases or sociopolitical orders: Spain and Brazil since the end of their last authoritarian regimes. We start in 1975, after the death of Francisco Franco, the Spanish Caudillo, and one year after the beginning of the distention process of the Brazilian military regime. Those years represent the authoritarian legacy in both countries and constitute the initial conditions upon

which their first intelligence agencies were created or uploaded. We analyze and assess the emergence of accountability mechanisms to oversee those agencies since the implementation of the first internal controls in the 80s, the latter institutional reforms in the 90s, to the external controls from Parliaments and courts in the first two decades of the 21st century.

In addition, we analyze and assess the accountability mechanisms that have emerged to the governance of personal data since the popularization of the Internet and the enactment of the first personal data protection rules in Spain in 1992. The changes brought up by the expansion of dataveillance, the business of data, and the forms to resist to that governance are also covered in the 2000s and 2010s. The year of the conclusion of this study is 2020. This year also serves as a temporal limit as the pandemic crisis of this year represent an important shift started in previous political transition in terms of management of populations and biopolitics. Yet, the analyzed phenomena and the accountability mechanisms continue to be performed after this date. In that sense, the final part of this study, regarding the meta-narratives of resistance and the futures of surveillance, is one attempt to analyze and map prospective trends on surveillance. We know that this gesture is very risky and not common to scientific studies, yet, we formulated theoretical principles that we believe should guide the evolution of accountability mechanisms in the times to come.

In both countries, we will conduct an exhaustive analysis of surveillance institutions and strategies. However, we do not aim to carve the field of democratization studies. For some scholars, the democratization process in both countries has ended. However, as expressed in the previous section, since accountability is one ingredient of every democratic effort, and provided that accountability is a continuous practice of everyday politics that must be improved, our understanding of democratization does not have an ending date or a final destination. In overall terms, democracy is valued by the democratization attempt to deepen and strengthen itself. In fact, democracy shares a not divine theological orientation that is shared with political projects from the Enlightenment era. In this work, democracy and accountability are not exclusionary, rather they complement each other. Assessing accountability would serve as an indicator to verify the state of art and the quality the democracy in both countries in the face of surveillance. However, we refuse to simply link this study with democratization studies, either in procedural or substantial terms.

This linkage would entail in creating categories and phases of democratic development as in the style of Tilly & Argilés (2007). From their perspective, there are four categories to democracy: high-capacity non-democratic state, low-capacity non-democratic state, high-capacity democratic state, and low-capacity democratic state. High capacity non-democratic states imply "little public voice except that allowed by the State; the broad presence of the state security forces in all public

policy; change of regime, either through a struggle between the elites or through a rebellion from below" (Tilly & Argilés, 2007, pág. 52). Whereas, high capacity entails "frequent social movements; the activity of interest groups and mobilizations of political parties, formal consultations (including competitive elections); extensive state monitoring of public policy combined with relatively high levels of political violence" (idem, p. 52). To those authors, the more democratic a state, the more citizenship takes the initiative to challenge the state and its institutions. The categories and division of democratic capacities and the intensity of the mobilization of political actors would be interesting to analyze accountability. Yet, as this study is focused only in two case studies, and presents a historical analysis of their accountability mechanisms, we prefer to cover several mechanisms to redefine surveillance in two dimensions (exceptional and normalized politics), leaving the door open to democratic studies in further studies. However, we do believe that democratic countries might and should improve accountability mechanisms in surveillance and beyond, either by institutional channels or by contingent practices from citizenship.

Furthermore, this work is skeptical about studies supporting democracy as a finished program that can be "installed" in every place. One can speak of formal democracies to refer to the contemporary forms of liberal government in western countries, but it is difficult to accept passively that those forms of government are automatically superior and represent democracy *per excellence*. And by liberal, we mean a tradition inherited from liberalism (see section 1.3) that defeated its previous competitors in the last century: fascism and real socialism. But liberal democracies are not the end of history (as in the style of Fukuyama (1989)) nor are final paradigms that cannot be improved in their internal logic. Accountability can foster and improve democratization, period. Whether this improvement can be taken to enhance liberal, radical, or alternative democratization processes is an open question. This potential would be a direction that must be interpreted by the reader and constitutes the focus of analysis in the final part of this study. Furthermore, according to the objective of this study, accountability will be worked in two directions: to guarantee and promote a degree of individual autonomy, and, to replenish the asymmetries of power between those who watch and those who are watched. Accountability, as mentioned, is the connector between authority and legitimacy, and this connection can be deemed as one of the substantial forms to perfect and improve politics because legitimacy cannot be understood without its major source: the general will of the people.

In different contexts, the objectives of surveillance are different. For example, if in the past surveillance was mainly attached to top-down institutional designs, especially in the field of intelligence, today the model of surveillance is also related to networks of governance between players from the state, market and international arenas (see Rodhes, 1997; Gill 2016). During the last century, surveillance was of especial interest to a narrower political "elite" in the conflict

between East and West in the Cold War. Nowadays, surveillance is still of interest for certain political elites, but now they share governance with other players in a diffused and broader surveillance realm in a more globalized world than five decades ago. To detect the differences in surveillance in each time and context, and to analyze our objects, this work is divided into two realms: 1) surveillance from intelligence security, and 2) surveillance of personal data. See *Table 2*.

Table 2: Two worlds or realms for surveillance analysis.

	Realm 1	Realm 2
Objects for analysis:	Main informational/ intelligence institution	Personal data networks on the Internet
Political category:	Exceptional-normalization	Normal-exceptionalism
Surveillance dimension:	Structural →Post-structural	Post-structural
Surveillance metaphor:	"Panopticon"	Rhizomatic "surveillant assemblage"
Watcher(s):	State intelligence agencies	Several data processors
Watched:	Target groups and individuals that in turn serve to regulate the whole population in a territory.	Data subjects whose information serves to regulate expressive groups of the population.

Source: the author

In the first realm, the object for analysis is the main strategic informational/intelligence institution in each country. This analysis starts in the late 70s as surveillance in this domain can be associated with the end of military regimes and their marks onto the new Spanish and Brazilian political processes. This realm represents the analysis of the exceptional-normalization category that was postulated in the second section. Compared with other policies and institutions, intelligence has "special powers" to guarantee the security of the sociopolitical order and achieve goals by non-conventional means. That is, intelligence services can adopt exceptional measures, like secrecy and confidentiality, to regulate and extract information from individuals. In that sense, in intelligence, the Schmittian exceptionality pattern has preeminence over the Foucauldian governmentality one to manage populations. Yet, both patterns appear not disconnected even in intelligence activities. Considering the theoretical discussion on surveillance, here we focus on the transition of a structural to a post-structural surveillance dimension. The Structural surveillance dimension can be associated with the characteristics of institutional centralization adopted in the times of the Franco regime and of the Brazilian dictatorship. The transition to post-structural surveillance means that the militarized regimes of exception have been replaced with the panopticon metaphor of surveillance in strategic institutions to the service of the state. In this realm, the aim is to verify how accountability has been worked to counterbalance or redefine intelligence practices in terms of

guaranteeing a certain degree of individual autonomy, including privacy, and to reshape the asymmetry of power between intelligence agencies and the whole population. It must be noticed that the whole population in each country has been indirectly regulated by targeting key groups and individuals through intelligence activities.

Besides, it is thought that some degree of asymmetric power is observable even nowadays in the intelligence realm. Notwithstanding, the fact that informational/intelligence services have had an important role in the transition of authoritarian regimes must be considered to answer how accountability has been implemented upon them. Assessing accountability in this issue is essential because it is known that the transition to a more democratic scenario in the late 70s was slow and regulated by security agencies in both countries, such as intelligence services. In short, this realm serves to analyze the surveillance panopticon scheme of a public and official gaze deployed upon certain individuals. To some extent, this gaze regulated the security of the socio-political order in new democracies according to the interests of state institutions. Thus, the lessons from the past are of importance to analyze and scrutinize intelligence activities. It is impossible to forget the deviations of power and the violation of rights that were facilitated by intelligence some decades ago. In addition, the evolution of these institutions matters to perceive their changes and continuities. Therefore, the past lessons of accountability in this paradigm are analyzed through a historical perspective that covers a time framework between 1975 and 2020. Moreover, if the scale of coercion, violence, and uncontrolled power has been reduced if compared to previous periods, intelligence agencies still have accountability duties and are important actors to understand surveillance nowadays. As the novelist John Le Carré, we still believe that intelligence services are "not an unreasonable place to look" and to explore a nation's psyche. For him, secret services are the true measure of a nation's political health, are "the only real expression of its subconscious."[4] For us, Le Carré statement is true, even when intelligence cannot be simplified to secrecy. Yet, the subconscious expression of a sociopolitical order is broader than the intelligence domain and needs to be analyzed in a second realm.

Whereas the object for analysis in the first realm are informational/intelligence agencies, the object in the second realm is "personal data surveillance networks" on the Internet. Here, a new fragmented and diffuse ground has risen since the late 90s to complement the previous realm. In this ground, surveillance practices have spread their objects, methods, technologies, purposes, and scopes. The official "gaze" of the state is not sufficient to understand the completeness of the surveillance society. Therefore, we focus on personal

[4] Jacobson, G. 2016, October 7. 'Snowden vs. Le Carré.' *The New Republic*. Retrieved from https://newrepublic.com/article/137557/snowden-vs-le-carre

information that is gathered, stored, and processed by several political players to create biopolitics through the Internet. This realm represents the analysis of the normal-exceptionalism category that was postulated in section 1.2. In personal data, normal-exceptionalism is related to a higher presence of governmentality to manage populations, although exceptionalism is also present to regulate individuals. Moreover, in the last decades, the management of personal data is not centralized in a few groups or institutions and is conducted especially through digital electronic tools. Hence, personal data on the Internet serves to understand the evolution of governance and the creation of a more fragmented surveillance society. In that sense, and considering the theoretical discussion on surveillance, this realm serves to analyze the liquid or rhizomatic metaphor that reminds the surveillant assemblage. Instead of focusing on a single institution, here we focus on the networks of governance to manage personal data on the Internet to analyze new accountability mechanisms. Provided that personal data is a piece of information extracted from an individual, that piece must be considered as a strategic component of one person instead of his/her ontological image or essence. Personal data can be interpreted by philosophical terms (as the abstraction and the identification of the "self"), by technical means (such as analogical registers, digital codes, and fragmented information from a data subject), judicial means (for example, separating the owner and the processor of this data, and creating rights for consent and deletion of personal data). In this work personal data is identified with key information handled by data processors in an array of governmentality practices related to biopolitics. Hence, this part aims to answer whether the management of personal data (in legal, market, and societal domains) is permeable to accountability mechanisms that can redefine the autonomy of data subjects. In other words, we aim to answer how data processors have been accountable for their actions regarding the information they manage from considerable groups of people.

In addition, this realm serves to analyze accountability in an asymmetric relationship between data processors and data subjects. Instead of having the past as the main reference to analyze surveillance as in the case of the first realm, the power relationships between watchers and watched in personal data matters if we look into the future. A more horizontal relationship between data processors and subjects matters to avoid that the asymmetry of power does not collapse into a de facto struggle to survive in regimes where different players (from the state, market, and civil society) promote pathological biopolitics and disgusting surveillance. If the authoritarian legacy (still) casts a shadow over intelligence institutions, in the case of personal data the question consists of avoiding new forms of liquid authoritarianism, systematic implicit coercion, and dystopian futures. Many dystopias from media and culture have a message on this, such as artificial intelligence being more humanist than human beings (*Blade Runner*, 1982), electronic and ubiquitous surveillance to predict crimes everywhere and at

the expense of privacy (*Minority Report*, 2002, and *Person of Interest*, 2011), technologies created with good intentions but used to harm people or classify them as mere objects (*Black Mirror*, 2011). Those narratives, either simplifying or exaggerating the reality of surveillance, serve as warning messages that alert us to avoid worst-case scenarios, and what is more important, they offer skepticism to understand and accept passively our condition as data subjects.

To verify our hypothesis, this work adopts a holistic approach to analyze the accountability mechanisms of surveillance. As expressed in the theoretical framework, accountability is a relational concept that consist in "who" is accountable, "to whom" one group is accountable, "about what" the accountability consists of, what is the context of accountability (why, where and how accountability is performed) and what are the results of the accountability. We operate those dimensions alongside the two realms to assess accountability outputs and to verify whether they answer the thesis objectives. The operationalization of accountability in the surveillance realms is summarized in tables 3 and 4.

Table 3: Operationalization of accountability in the first realm.

Accountability dimensions	Realm 1	
	Spain	Brazil
Who is accountable?	National Intelligence Agency	National Intelligence Agency
Time span	1975-2020	1974-2020
To whom it is accountable?	- To internal controls - To legislative control - To judicial control - Due to international intelligence cooperation - To media and society	- To internal controls - To legislative control - To judicial control - Due to international intelligence cooperation - To media and society
About what it is accountable?	Actions developed by strategic and security intelligence that monitored or collected information of key groups and individuals	Actions developed by strategic and security intelligence that monitored or collected information of key groups and individuals
Why/where/how is accountable? (context)	To be analyzed through a historic perspective and case study at the national level	To be analyzed through a historic perspective and case study at the national level
Assessing accountability according to its internal principles	Did the accountability action result or promote at least one of the following principles? -Responsibility -Transparency -Answerability -Enforcement (punishment)	Did the accountability action result or promote at least one of the following principles? -Responsibility -Transparency -Answerability -Enforcement (punishment)
Assessing accountability according to our thesis objectives	a) To redefine the management of subjects autonomy, b) To redefine the asymmetries of power between those who watch and those who are watched.	a) To redefine the management of subjects autonomy, b) To redefine the asymmetries of power between those who watch and those who are watched.

Source: the author.

In the first realm, we focus on the evolution of the national intelligence agencies in both cases. In the Spanish case, we analyze the evolution of the main institutional nodes that exercised domestic intelligence and counter-intelligence tasks in each country since the democratic transition. In Spain, the institutional evolution evolves three changes: The Central Documentation Service (1972-1977), transformed into The Superior Center of Defense Information (1977-2002) that, in turn, became The National Intelligence Center (2002-nowadays). In Brazil, the intelligence institutional evolution at national level started with The National Information Service (1964-1990), but we start the analysis since 1974 (year of the distention process of the military regime) followed by a period of reformulation and the creation of The Brazilian Intelligence Agency (1999-nowadays).

Since their creation, those agencies have reported their decisions and activities to other players in order to show accountability. Those players are located within the executive government (internal control), they are controlled by the legislative and judicial power, as well as they can be monitored by extra-state domains such as media and the civil society. As intelligence services have their activities protected by official secrecy, it is difficult (sometimes impossible) to know exactly what they are accountable for. Some clues about their accountability and performance are given by the role of media and groups that have worked in those institutions. These reports are considered as auxiliary tools to reconstruct the activities of the intelligence services but they must be interpreted carefully and with a certain degree of skepticism. Yet they are important sources to assess accountability beyond official discourses and narratives. Another domain in which intelligence agencies need to show accountability is cooperation with third states and groups at the international level. This domain is under-explored in both cases and is essential to assess intelligence activities in times of globalized cooperation and international convergence among surveyors to respond to threats to states.

To analyze and assess accountability, we show the institutional evolution of intelligence, the main players to whom they were accountable for, and the context of this accountability. That is, in each moment and place, accountability was conducted after political transformations in the sociopolitical order, international pressures, professional demands, justice clashes, scandals, whistleblowers, and so on. All of those motivations are to be depicted and inserted in their specific time and circumstance. Therefore, to assess the accounts given from intelligence agencies to distinct players, we evaluate how accountability was performed according to its context and whether that performance resulted or promoted at least one of the theoretical principles that were expressed in the previous section. An ideal accountability action evolves several principles such as responsibility, transparency, answerability, and enforcement. However, historical contingency and constraints factors can affect the performance and the presence of those principles. For instance, transparency and enforcement from/over intelligence agencies are scarce and difficult to be achieved most of the time. But it does not

mean that other principles can be moved to promote accountability. Besides, the mere presence of all of those terms does not define a good or a bad account. Of course, the presence of only one of those components implies poor accountability performance. Thus, the key point consists in assessing the presence and the quality of those principles in diverse accountability actions and times.

Alongside the accountability analysis of intelligence, we will evaluate this realm according to the thesis objectives: How accountability of intelligence agencies redefines the management of subjects' autonomy? And, how the accountability efforts were/are capable to transform the asymmetries of power between those who watch and those who are watched? We have already explained the definitions of subjects' autonomy and asymmetries of power. In terms of watchers and watched, traditionally intelligence agencies have deployed surveillance over certain targets and groups, instead of watching the whole population in a country at once. Yet, by deploying an exceptional gaze to watch some individuals (like intrusive methods and informants to collect sensitive information), those agencies turn out to create the conditions to regulate the rest of the population insofar as governmentality measures are not disconnected from exceptionality. Surveillance is not limited only to the targets, to suspects, or criminals. The panoptic metaphor works thanks to the auto-discipline or self-vigilance that the rest of the population adopts in the face of the watchers. Thus, the effects of surveillance and intelligence are not restricted to certain targets. Indirectly, these activities also create biopolitics and turn out regulating the whole population, especially in the name of security. At this point, accountability matters to redefine the intelligence potential to manage populations. In that management, intelligence agencies do not exist in a political vacuum; they cooperate with other security institutions and report to higher policy-makers in each country. The assessment of accountability between those agencies and other political players, therefore, gives us some clues to identify the capabilities and limits of those agencies when it comes to sharing their products (intelligence outputs) with other institutions. Finally, it can give us a basic idea about one important realm (intelligence), which in turn is part of a broader surveillance puzzle.

Table 4: Operationalization of accountability in the second realm.

Accountability dimensions	Realm 2	
	Spain	Brazil
Which kinds of social domains are important to redefine the governance of personal data?	-Legal scope (European and National) -Market scope -Citizen agency scope	-Legal scope (National) -Market scope -Citizen agency scope
Time span	1992-2020	1999-2020
About what organization in each domain are accountable?	About the bulky collection, transference, and process of personal data that was collected directly or indirectly on the Internet	About the bulky collection, transference, and process of personal data that was collected directly or indirectly on the Internet.

Why/where/how those groups are accountable? (context)	To be analyzed through governance strategies in each country	To be analyzed through governance strategies in each country
Assessing accountability according to its internal principles	Did the accountability action result or promote at least one of the following principles? -Responsibility -Transparency -Answerability -Enforcement (punishment)	Did the accountability action result or promote at least one of the following principles? -Responsibility -Transparency -Answerability -Enforcement (punishment)
Assessing according to our thesis objectives	a) To redefine the management of subjects autonomy, b) To redefine the asymmetries of power between those who watch and those who are watched.	a) To redefine the management of subjects autonomy, b) To redefine the asymmetries of power between those who watch and those who are watched.

Source: the author

In the second realm, we focus on personal data networks on the Internet. As this paradigm refers to a liquid surveillant assemblage, the attention goes to strategies to process personal data in different domains. Thus, we adopt a policy network analysis to study the governance of personal data in different social domains: Legal regulations, market scopes, and civil agency scopes. The domains serve as components to depict a broader image of data processors and surveillance. Yet, by analyzing the strategies to process data in each domain, we also want to verify the efficiency and limits of accountability on a macro-social scale or at the state level. We have chosen personal data gathered on the Internet insofar as most of the digital content from individuals (images, voice, messages, calls, texts, and other platforms) is uploaded and downloaded from the Internet. Other forms of ubiquitous surveillance such as CCTV images, GPS position systems, and genetic databases are of importance but they remain outside this study. In the World Wide Web, different kinds of information are transformed into texts and codes. These codes represent and translate individualities to the digital world. At the same time, they frame the world towards individuals. Since we are focused on the Internet as a platform that allows the communication and transformation of huge amounts of personal data, the temporal framework of this realm begins in 1992. This was the year when the first data protection Act was promoted in Spain and symbolizes the start of a decade when computing machines and Internet users increased exponentially in both countries. However, historical analysis is replaced by a policy network analysis to assess accountability in both countries. In this analysis, there is no intention to create a fixed image regarding accountability strategies and political players. Rather, we are interested in how surveillance can be redefined by accountability continuously in a dynamic governance model.

To assess the accounts given from data processors we adopt the same criteria of the first realm. We evaluate whether the accountability performed in a specific domain resulted or promoted at least one of the theoretical principles that were expressed in the previous section. That is, the point consists of assessing the presence and the quality of accountability principles (responsibility, transparency, answerability, enforcement) between distinct players in a social domain. Moreover, we will evaluate accountability in terms of the thesis objectives: How accountability in each domain serves to redefine subjects' autonomy? How accountability efforts replenish the asymmetries of power between data processors and data subjects? Data processors deploy surveillance tools with an array of purposes that most of the time is far from exceptional trends. Aside from Law enforcement, many of the activities to process data are related to governmentality cases such as running a company, buying services, complaining against bureaucracies, supporting an idea, sharing our thoughts in social networks, and so on. Thus, instead of watching the whole population in one country at once, data processors are concerned about specific practices and population profiles. But the fact that they deploy governmentality dispositives to watch certain individuals does not mean that those tactics cannot be associated with exceptional measures. When different personal data fragments are joined, they can create a valuable source for other surveyors like security agencies and market companies. In that sense, normal forms of surveillance can enable the conditions to regulate broader populations by governmentality tools that are not disconnected from exceptionality. Surveillance is not limited only to the targets or persons of interest. The rhizomatic metaphor in this realm works thanks to the remote connection between the array of rhizomes in the surveillant assemblage. Indeed, some rhizomes are more powerful than other ones and gather huge amounts of personal data. Those big data processors, which have more potential to surveille considerable parts of the population like Google and Facebook, are of interest to our analysis. In this realm, accountability matters to redefine the role of personal data processors to manage groups of the population. In that management, individual autonomy and privacy are essential to avoid pathological forms of surveillance. Furthermore, they matter to avoid that the political distance between powerful data processors and data subjects increases to the point in which the future surveillance assemblage collapses into a cage of subjugation, lack of public legitimacy, or disgusting politics.

We have explained the operationalization to manage and assess accountability in this work. Now is time to explain how we structure the overall thesis dissertation in terms of methods, information, and techniques to validate our information. The technical information of the thesis dissertation (see Table 5) is crucial to understand and interpret our work as well as its cognitive limitations. In that sense, we have already mentioned that our objective is to assess the evolution of accountability mechanisms in surveillance practices. As secondary

objectives, we want to verify how accountability can redefine surveillance in terms of the management of subjects in a specific population, and how accountability can redefine the asymmetries of power between those who watch and those who are watched.

As research methodologies, we adopt a different approach in each realm. In the first realm, as we want to assess accountability mechanisms in a "panoptical" surveillance domain, the approach is a case study research. The case study consists of a methodology of empirical research (Yin, 1989) (Eisenhardt, 1989) that mainly adopts qualitative techniques to analyze a real context, and uses multiple sources of evidence with inductive or deductive scientific approaches (1994). In short, a study case analyzes a certain object or a certain unit to examine its internal logic and external relations. In this work, the units for the case study are two intelligence institutions, one in each country. These units are understood as the main nodes for security intelligence since the democratic transition in each place and serve to analyze how accountability was performed according to their political context. Thus, those institutions are divided according to a longitudinal historical perspective and sub-divided into aggregated domains or pieces that can be joined to construct a bigger puzzle: intelligence communities. That is, by using a simple unit of analysis (intelligence institutions), it is possible to follow the evolution and changes in broader intelligence communities at the state scale. In this evolution, the analysis of cases is oriented by neo-institutionalism and legacy constraints theoretical grounds. This means that the intelligence institutions were constructed upon specific historical institutional lines that guided their evolution and power. The backgrounds of those institutions matter insofar as they shed light upon critical moments of the political transitions and explain the present institutional designs and legal configurations. At the same time, the contingency of each country could have exercised a constraint or an opportunity to those institutions in terms of surveillance. Those specific moments serve as points for change and continuity that some organizations use either to reshape their position or to consolidate power in the face of other political players and within an organizational community such as intelligence.

In the second realm, as we want to assess accountability mechanisms in surveillant assemblages, the approach should rely on the political interaction among distinct players instead of focusing our analysis on a single institution. Thus, a governance policy network analysis seems to be accurate to identify, examine, and assess accountability produced by an array of players that interact in broad communities. According to Volker Schneider, the common denominator of the policy network analysis is that the formulation of public policies is no longer attributed solely to the action of the state or a singular and monolithic actor. This results from the interaction of many actors, including the private and social sectors. The concept of the network refers to direct and indirect links between actors that are involved in the formulation of policies. Although many actors are

involved, there is a difference in power and influence between them. Positions of power are not determined only by status but also through informal links (eg, communication, resource sharing, strategic interaction) (Schneider, 2005, p. 38). In light of that, governance policy network analysis is the approach that enables to assess how personal data serves to surveillance and how it is processed in different social domains (State-rooted regulations, market strategies, and civic agency). To assess the networks of personal data in each country, we adopt the analytical tools by Scharpf (1997). This author proposes a situational logic in which each public policy establishes a system of sociopolitical interaction by different resources at the disposal of the actors, a structure of opportunities, and specific institutional settings that shape the development of certain modes of interaction. The basic elements of the analytical framework proposed by Fritz Scharpf are the following: a) To Identify actors as well as their preferences, perceptions, and abilities; b) To identify institutional frameworks and rules that delimit courses of action; c) To frame a constellation of actors to a specific moment or issue, and d) To analyze the modes of interaction in constellations located in specific institutional frameworks. This study focuses especially on the second and fourth points. As this study is exploratory, and since the identification and delimitation of a surveillance community involve thousands of groups and organizations that change continuously in each country, we focus on identifying the institutional lines that affect the entire constellation of actors and the strategies they adopt to interact among them. In other words, instead of identifying the exact position of the pieces in the surveillance game and the size of the board, the policy network methodology in this realm is mainly (but not only) used to understand the rules of the game and the movement of the pieces in the board. Other scholars have proposed other analytical tools, such as Marsh & Smith (2000). However, the focus relies on the interactions of different political actors due to the relational nature of our central concept –accountability- and because of the fluid strategies to process personal data. Hence, in this realm, since we cover different social domains and interactions, it is possible to suggest that there is a holistic view to analyze specific units (personal data processors) in each country.

As study cases to assess the accountability of surveillance, we have chosen Spain and Brazil. As a starting point, the author of the study has researched and worked in both countries, owning certain expertise and analytical potential to formulate situated knowledge and to conduct an immersive cultural and social study. Notwithstanding, those reasons are not enough and the selection is explained also because both countries initiated a political transition after authoritarian regimes at the end of the last century, specifically, after 1975 in Spain and 1974 in Brazil. Those regimes left marks in terms of the administration of subjects, surveillance capacities, and in the relationship between authority and legitimacy in the current political landscapes. In that sense, some scholars even mention that those cases can be inserted in the third wave of democratization

process initiated after World War II. That is, they depended on the domestic and the international dimensions to initiate and consolidate political modifications in terms of structure, institutions, and culture. At the same time, those countries replenished the ideas of political transition in Europe and Latin America and beyond. Both Spain and Brazil can be understood as cases of arranged transition, as the pace and intensity of the democratization process were controlled by the civic and military elites. These countries are deemed as cases of slow, secure, and incremental transition into a more democratic scenario, especially in terms of culture and substantial democratic values (Numeriano, 2007). Thus, accountability, a substantial process that redefines the idea of authority, is supposed to have similar yet distinct paths in terms of evolution, implementation, and impact in both countries, justifying their use for study cases. In that sense, instead of considering two similar cases, we preferred to elect two cases with a certain level of likeness but distant in terms of polity (a quasi-federal parliamentarian monarchy against a federal presidential republic) and socio-geographical location (Southern European and European economic and security complex vis a vis the South American and Western Hemisphere security complex, to use the terminology of Buzan (2003)). That controlled difference allows us to analyze accountability and postulate general theoretical propositions insofar as our selection contemplates a variance of mechanisms that could be useful for a broader sample of countries, especially to other European and American cases, but not only. Finally, Spain and Brazil are important cases in geopolitical terms as their intelligence services and strategic information are crucial pieces to complete the puzzle of security alliances, political cooperation, and economic governance in their respective continents. Either in terms of political stability, energetic sources, internal gross domestic product, predisposition (or not) to abide by democratic standards, active citizenship, all those terms help to enrich the analysis and objectives of this study.

The study is descriptive, exploratory, and explanatory. According to the acknowledged classification of Yin (1994), the objective of one research can be of three types: 1) Descriptive: to depict the object of study or to present a complete description of the object of analysis concerning its real context; 2) Exploratory: to discover aspects and formulate questions that determine the viability of investigation procedures. This type validates existing methods or redefines the theoretical framework to analyze a certain phenomenon. This type is used, for example, in pilot projects. 3) Explanatory: To analyze cause-effect relationships, and explain causes and effects. For example, explanatory research is commonly used to clarify why and how a certain phenomenon occurs or to test a theory. Besides, it aims to the development of new theories and to open new paths for research.

We believe that this work involves the three points stated by Yin due to the methodologies adopted in each realm and because this study aims to produce new

theories or theoretical instruments to analyze accountability and surveillance practices that are not restricted to the selected cases. Besides, this work uses a qualitative analytical induction approach (analytical generalization) and a deductive process (theoretical propositions), especially in the last part. In that sense, our kind of samples is two national intelligence institutions (Realm 1) and two personal data networks (Realm 2) that are disaggregated in several social domains in which data processors interact and show accountability. Because of that approach, the samples of analysis are not random neither they follow a sampling method. Rather, the selection follows logical and theoretical criteria as expressed above. Moreover, the criteria are related to the discussion conducted in the theoretical framework and to the operationalization mentioned in tables 2 and 3. Although the analysis of those samples could enable an analytical generalization for other cases and national contexts, there is no aim to establish statistical generalizations.

The reader of this work will find information related to social sciences, humanities, arts, natural sciences, computing studies, and other fields. The methods to collect information and evidence are based on the review of literature and documents (legislation, briefs, reports, and official publications) related to our objects. Moreover, we review press articles stored in a database that contains information from different newspapers and journals in each country (see section 3.8 in Chapter 3). The sources of that information are from internal and external scopes concerning our objects. By internal scope, we mean documents and multimedia sources (web pages, texts, images, photos, tables, internet applications). The information given was available in public domains or made public by key informants. In the case of intelligence, no confidential information, official secret, and sensitive data were received or demanded from our objects. Secrecy is one important characteristic that intelligence researchers face to analyze this realm. Notwithstanding, the analysis of the political interactions within the intelligence community as well as the accountability for the public can be achieved mobilizing other accountability principles beyond transparency. Thus, transparency must not be a permanent obstacle to research this matter. Furthermore, to overcome this limitation, we used external information sources such as specialized publications and pertinent literature from our cases as well as from international countries. Besides, we contrasted narratives and reports from official organizations with unofficial narratives, for example, with media and press articles in order to add more perspectives in the validation of information sources. The reversal was also true, as media and press articles were contrasted with legislation and other official sources.

In that sense, the internal and external validation of the information sources is made from the beginning to the end of this work. On the one hand, we validate internal information by following a coherent pattern: first, an object should not contradict itself internally or in its internal logic; second, when it happens,

incoherent patterns and contradictory information stemmed from the same source are linked with an explanation, a systematic comparison with the specialized literature and the theoretical framework. The linkage with the explanations does not intend to clarify the contradictions of content; it serves as a validation method to clarify the position of one source in light of other ones. On the other hand, the external validation is produced by contrasting our cases with other ones and by expressing the results obtained in that association. However, there is no intention in doing a comparison per se or use a set of methodologies from political comparison as we adopt a case study and policy network analysis. The results or conclusions enable literal and theoretical replications. That is, they can foresee similar results for other cases in processes where the theory is supposed to predict similar results in similar contexts, but they also can predict contradictory results due to predicted reasons (cases where the theory can explain different but predictable results in no null hypothesis). In both cases, the quality of the validation relies on cross-reference analysis of different sources (in the case of intelligence this could be a challenge), the context of production of those sources, the context of their representation in this work, and the context of the reader. As every textual, scientific, and cultural production, this study closes the hermeneutic cycle by establishing an interlocution with different audiences: the universe of this work.

The universe of the work means that there is a group of people to whom this text is directed to. As a matter of fact, this text is oriented to general people interested in politics, society, and culture. This dissertation is a product of a commitment to the study of History and Political Science, the fields in which the author developed his academic formation. As mentioned in the preface, this research also supports an interdisciplinary convergence to produce synergic and coherent knowledge that should be of interest to the mentioned fields plus Sociology, Philosophy, Law, Economy, Psychology, Communication, Journalism, Social Movements, Cultural studies, Literature and Narrative studies, Arts and Aesthetics, Computing Science, Informational Systems Engineering and other ones. In different stages of this work, those “traveling fields” have redefined the writing, the theoretical ideas, and the objects for analysis (Bal & Marx-MacDonald, 2002). This not consists of adding different fields by random criteria, but in producing a theoretical framework to conduct empirical analysis and to formulate overall propositions, as summarized in the conclusion. We hope that this work can foster connections among historical, political, moral, cultural, cognitive, and technical professionals interested in surveillance studies and beyond. This work also formulates recommendations or general ideas at the ending part of each section. Thus, it hopes to be useful to practitioners and non-practitioners in each field. Yet, if we need to restrain the universe of this work, we can affirm that the results are oriented especially to intelligence and security organizations, market data

processors, civil society organizations, and the academic sectors that are present in at least one of the countries of analysis but not only.

Table 5: Technical information of the thesis dissertation

Main objectives	To assess the evolution of accountability mechanisms in surveillance. To verify how accountability can redefine surveillance in terms of the management of subjects in a specific population. To verify how accountability can redefine the asymmetries of power between those who watch and those who are watched.
Research methodology	Case study research aggregated perspective for a single unit of analysis (Realm 1), Governance Network analysis, holistic perspective for different units of analysis (Realm 2). Exploratory, descriptive, and explanatory study.
Analysis units	National intelligence agency (Realm 1) Personal data networks (Realm 2)
Geographic scope	Spain and Brazil
The universe of the research	Intelligence institutions, security organizations, market data processors, civil society organizations, academic researchers, the general public.
Sample type	No random samples and no sampling criteria. The selection is logical and theoretical. Samples could enable an analytical generalization for other cases although without statistical generalizations.
Samples:	Two national intelligence institutions (Realm 1) Two networks disaggregated in social domains in which data processors interact and show accountability (Realm 2)
Methods for collecting evidence	Review of the literature. Review of legislation, briefs, reports, and official documents. Review of press articles. Review of unofficial publications to contrast official information.
Information sources	Internal: documents and multimedia sources (web pages, texts, images, photos, tables, internet applications). External: specialized publications, reports from official and unofficial organizations, media database.
Analysis methods	Especially qualitative.
Scientific approach	Analytical induction (analytical generalization). Deductive processes (theoretical propositions).
Methodological evaluation and quality	Constructive, internal, and external validity. Theoretical, interpretative, and contextual analysis to reach reliability and consistency.
Research period	January 2017 – December 2020

PART 2

Chapter 3. Accountability in the realm of intelligence

The first objects in this study are intelligence agencies in Spain and Brazil. What is intelligence? Why the definition of this name? Who collects and how intelligence information is analyzed? These and other questions emerge when we consider this field. It is said that intelligence *is* information, but not all the information can be labeled as intelligence. Intelligence, in its arrays of forms, use specific knowledge to define goals, and convince or constrain the action of other players by soft and hard means. This chapter analyzes the theory and concepts of strategic intelligence related to internal security (section 3.1). After the analysis of intelligence, we depict the authoritarian legacy (section 3.2) and the institutional evolution of intelligence agencies in Spain and Brazil (section 3.3). Then, we turn to the different mechanisms of accountability in this realm: internal control (section 3.4), legislative control (section 3.5), judicial control (section 3.6), international oversight (section 3.7), the media role and society (section 3.8).

3.1. Intelligence

Intelligence arise from two core functions to sovereignty powers -foreign policy and war- in order to help decision making in high politics, such as for rulers, kings, and military commanders. Intelligence was like the eyes and ears of political elites and states (Cepik, 2003). Moreover, since the professionalization and specialization of this activity, especially after World War II, intelligence was framed the logic of giving support to strategic decisions based on sensitive information. Intelligence was interpreted as knowledge, as a process, and as a form of organization. The first means that intelligence is a refined knowledge that is essential to the very existence of state and to the foundation of a political order. A state cannot survive for long times with no specialized demand and consumption of aggregated knowledge regarding competitors and allies. Intelligence as a process consists of the methods and forms to collect and transform raw information into a valuable form of knowledge. Finally, intelligence as an organization refers to the creation, specialization, and professionalization of certain institutions to deploy channels to gather and process information.

If intelligence as a process is as ancient as the oldest states, intelligence as an organization has a more recent history. In that sense, the literature mentions the

creation and specialization of Anglo-Saxon agencies as cases that reformulated intelligence as an organization. This relates to the preeminence of western military forces during World War II and the Cold War. For example, a much-extended notion of intelligence for analysts and practitioners comes from the institutionalization of the Office of Strategic Studies and the theories developed by Sherman Kent. Kent was a historian and scholar that emphasized the vital importance of creating a methodology for performing intelligence analysis as a basic condition for its professionalization. Despite he did not create a doctrine and theory about intelligence, his work contributed to the transformation of the Office into the Central Intelligence Agency (CIA) from the USA, Kent guidelines served to replenish the approaches to collect information in the realm of national security based on scientific analysis and rational tools to interpret sources and objects (Kent, (1949) 2015).

Another important theorist, Mark Lowenthal, believed that intelligence can be conceived by the means information is collected, analyzed, and disseminated. For him, intelligence is also characterized by the types of covert action conducted and conceived (intelligence as a process). Intelligence can also be thought of as a result of this process (intelligence as a product). This part includes both the estimations and reports intended for the end-user, as well as the results of covert actions and measures to neutralize the opposing intelligence, called counterintelligence. In this case, the most common techniques are blocking access to information or false disclosure, deceiving the adversary through the so-called counter-information (Lowenthal, 1993).

Kent and Lowenthal also formulated the acknowledged “cycle of intelligence”. This five-step cycle is initiated in a phase called “Planning and direction”, a moment when the organization guides the internal actions according to policymaker demands. The following step, “Collection of Information” relates to specificity, typology, and instruments at the disposal of the organization to extract information. HUMINT, SIGINT, IMINT, FININT, OSINT are just some examples of the methods and channels to collect information, such as human, electrical signs, images, and aerial photography, financial records, and open-source information, respectively. A third step called “Processing” involves converting the vast amount of information to a form usable by analysts through decryption, language translations, and data reduction. The following step, “Analysis and production”, includes integrating, evaluating, and analyzing all available data -which is often fragmentary and even contradictory. Analysts are to consider the information's reliability, validity, and relevance to construct an informational product: intelligence. This product is supplied to policymakers and supervisors in a step called “intelligence dissemination”. The products are briefs and reports delivered to the same decision-makers of the first step, who in turn might reinitiate the cycle.

The classical intelligence cycle resembles Fordism division of work in contemporary organizations. The sequential logic was criticized because it contains a rational and linear approach to interpret social reality. As in the case of policy studies that analyze their targets by sequential steps (definition of agenda, decision-making, formulation and implementation, evaluation), the intelligence cycle is influenced by its origins in top-down organizations and by a programmatic logic to construct a political agenda and collect information. Alternative models to analyze public policies, such as the "garbage can" model, the incremental model, and the backslash effects – that also consider contingency and irrational dimensions to analyze the social reality- challenge the linear vision of a sequential cycle to understand and solve problems. In that sense, alternative models such as a "Target Centric Approach" can be understood as a post-Fordism attempt to update the intelligence cycle. In this approach, the cycle can be viewed and analyzed from three perspectives: structure, function, and process. Structure describes the parts of the whole organization, emphasizing people who are part of the organization, and their relationships with one another as part of the whole. Function describes the product of the organization and emphasizes decision-making. Finally, the Process describes the activities and knowledge to formulate the final product. An analyst must consider each of these components at the same time and in a dynamic form while examining a particular target or organization.

> The target-centric intelligence model corresponds to the definitive incorporation of business management techniques. This allowed the evolution of the intelligence cycle, based on a binary mechanism of questions and answers, which consisted of pondering and acting. In this case, there is a constant and linear movement of the question to the answer. […] Instead of a set of predefined actions distributed in a compartmentalized work by several agents, a collaborative work constantly uses information and establishes communication between producers and users (Carpentieri, 2016, p. 103).

The target-centric approach is similar to flexible small-scale organizations that exchange information to solve a problem, rather than a colossal bureaucratic sequential cycle by professionals who specialize in distinct processes. Yet, this kind of approach has been criticized for demanding more time to deliver the intelligence products for policymakers than the traditional cycle (Johnston, 2005).

The cycle of intelligence is a form of collecting data. However, this process received other names in the past. In our cases, the word "intelligence" appeared only in the recent institutional reforms of agencies at the beginning of this century. Before, the common word that described the collection of sensitive information by the states received the vague name of "information" or "information services". The etymology of the word "intelligence" is not clear, but it appeared since the reform of defense agencies in the United States, in United Kingdom and at the first stages of the Cold War.

The use of intelligence replacing the word "information" could be interpreted in a Foucauldian dimension. That is, even language and the use of certain vocabulary is a dispositive that ensembles the distribution of power showing the form in which a certain organization presents itself to other ones. In Chapter 1, we have shown that disgusting politics might be covered by layers of "beautiful" terms, such as aerial non-tripulated vehicles to describe bombing drones. One can even mention the acknowledged phrase "elements of massive dissuasion to keep the peace" to refer to nuclear weapons. In that sense, the case of "intelligence" is also paradigmatic in the use of language. As the institutions who collected sensitive information changed their methods and tried to erase a reputation based on abuses of power –especially in Spain and Brazil- it was necessary to replace their work with a word used by the best institutions of this field in the world. Here we can verify the Anglo-Saxon influence over security institutions to share a term to describe their information activities. The word intelligence suits a grammatical differentiation and a praxis that complemented but was different from traditional activities like the military and police to guarantee the security of the state.

In a Derridian approach, the term "intelligence" also enhances an action that reinforces rationality and efficiency. As synapses and neurons processing signs from terminals in a body to assure the continuity of the live form, the information process created to preserve the survival of the state is allegoric to the unidirectional flow of information from terminals to the "head". This activity reminds the cognitive and superior "thinking" part of the political order who decides about the collection and dissemination of useful information. By using the term "intelligence" instead of information, data, or knowledge, this activity acquires an "unquestionable" connotation to support and orient policymakers. "Intel over the terrain says that..." or "our intelligence services believe that the risk of…" entails a solemnity that needs special attention by policymakers. We can see how the guardians of the state use language to preserve and consolidate a privileged space of power when compared to other public institutions and security organizations.

Even when this field has an implicit logic of high-quality standard to process information and create secret products to privileged consumers, the intelligence activity still appears to lack a definition and a doctrine. Gill & Phythian (2016) differentiate intelligence as an object, as the "what" question, from the array of fields and connections that intercross intelligence. Regarding the "what" question, they mention that intelligence, at the beginning of the Cold War, was related to secret activities. Intelligence was/is "targeting, collection, analysis, dissemination, an action intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities" (Gill & Phythian, 2016, p. 6).

Furthermore, Shulsky & Schmitt (2002) express secrecy as the distinctive and fundamental element of intelligence, to the point of identifying it with a state of silent warfare. In turn, Herman (2013) points out that secrecy is the base of all relations of intelligence, either concerning the government, or the image of projected to society. The need for secrecy leads to a series of procedures within the state, involving prohibitions and formalities to preserve secrecy. Thus, it is common to attribute to a certain authority the power to classify the product, based on gradual levels of stealth. The purpose is to prevent certain sources, certain materials, certain decisions, or operations from coming to the public knowledge as this eventually might cause damages to the interests of the country or the organization.

We can see a line of continuity between strategic intelligence and national security. Intelligence is the secret and exceptional measure to guarantee the Raison D'état. It is the core and exceptional pillar to sustain a political order in the face of other competitors and threats. To achieve that, powerful intelligence agencies have even exercised influence by using force, through promises of wealth or threats to bankrupt, or social and political pressure, especially during the Cold War (Garthoff, 2004). The fact that so many novels, films, news in graphic and written culture have dedicated attention to this realm, thus, must not be of surprise. For example, in the case of Spain, Matey (2010) notes a similar increase and interest in this realm since the end of the Cold War. Earlier work was dominated by history and military studies, reinforced by books on intelligence scandals in the 1980s and 1990s. He suggests that there are four approaches to intelligence in Spain: the historical-military approach, the journalistic approach, the economic, and the international relations/political science (including philosophy and law) (Matey, The development of intelligence studies in Spain, 2010).

In the case of intelligence studies as a discipline, Farson, Stafford & Wark (1991) reflected on the state of Intelligence Studies (IS) identified eight approaches to the study of intelligence: the research project; the historical project; the definitional project; the methodological project (applying social science concepts to intelligence); ethnographic memoirs; the civil liberties project; investigative journalism; and the popular culture project. In turn, drawing on other scholars, Gill & Phythian (2016) have identified four main areas of work: research/historical; definitional/methodological; organizational/functional; and governance/policy. Archivist, historians, theorists, and other scholars that take intelligence as their object and field of analysis cover the first two areas. Meanwhile, practitioners, analysts, professionals, and bureaucrats within intelligence organizations cover the last two areas.

The research/historical work was the first one to boost intelligence as a field of study as many historians were concerned in the revelation of key aspects of intelligence agencies, such as the role in military campaigns during the two World

Wars and later conflicts. This work is illuminated by the declassification of secret material and the investigative work with analysts in formal and informal ways. In addition, the definitional/methodological field of studies has obtained importance but still orbits in the Anglo-Saxon sphere of influence in terms of research and publications. In this field, fifty years ago, an "identity crisis" emerged as some authors such as Klaus Knorr expressed that:

> "There is no satisfactory theory of intelligence – neither a descriptive theory that describes how intelligence work is actually performed nor a normative theory that attempts to prescribe how intelligence work should be conducted. […] There are beginnings and fragments of such theories […] but a fully developed theory or a set of theory does not exist (Knorr, 1964, p. 26).

At that time, intelligence theory wanted to constitute itself as a new field of knowledge that draw but was not subordinated to social sciences, political science, and organization theory. More recently, the definitional/methodological field has moved from a unique theory about its nature and epistemology to a more open approximation to different objects (intelligence analysis, counterintelligence, foreign intelligence, military intelligence, etc.), that draws and is enriched by other social sciences more organically. This shift is explained by changes regarding security and threats to the state in the vision of public officials as well as due to the overlapping nature of social phenomena in the vision of the analyst. Despite the growing volume of publications and briefs, some keys aspects inherited of the foundational cycle of intelligence and its specific nature still prevail: Intelligence is different from the 'knowledge management' that is the bedrock of all state and corporate activities. Intelligence key factors are still security, secrecy, and resistance (from targets and competitors). Those key aspects establish a fundamental difference between intelligence and, for instance, the more general "risk-assessment" process that accompanies every company and corporation (Wilhelm, 2002).

The organizational/functional field, meanwhile, is focused on comparing intelligence institutions with other state bureaucracies. Here the element of secrecy emerges to isolate and create a specific organizational environment that will determine the methods to collect, process, and disseminate information. This field is also concerned with normative principles such as efficiency, professionalization, and cooperation among intelligence organizations and extra-state actors. As Hill observes, few organizations change themselves easily and, if reform or regression takes place, it is very likely to be the result of external pressure from other, government or civil society, actors. These changes and pressures are the subject of the fourth field: governance/policy. In this field, the key question is related to the intelligence impact on government and what impact does the government has on intelligence. However, this question can be extended

to a mutual impact between government –mediated by intelligence agencies- and society, as we will show in our study cases.

In the governance/policy field, the impact between intelligence and government, or between government and society, is reflected, for example, on the relationship between practitioners and scholars. In that sense, there could be mistrust from the practitioner community towards academics and, in many countries, there is minimal contact on what does occur within the former community while mystery and suspicion awake in the latter group. Aside from the expected secrecy that surrounds intelligence, many practitioners might not speak and be as accountable as other officials of government. At the same time, many scholars will not approach to analysts as their work, names and sources are classified by official regulations. For those motivations, the contact between both practitioners and scholars use to be informal or established in a para-psychiatric fashion. That means, the scholar dedicated to intelligence analyze his/her object by indirect contact with the subconscious part of a state institution. He or she needs to build a "diagnosis" about the archetype of one organization based on fragments, secret information, and even contradictory data obtained by indirect ways and with no direct knowledge of the work being developed in the inner ego- the intelligence organization. Meanwhile, the analyst and intelligence official cannot establish direct communication with the therapist, the scholar, as it would be considered a *paria* for violating an internal code that rules the intelligence community. For those reasons, it is difficult to assess and recognize the real virtues and deficits of the intelligence work developed in a country. It is said that this profession has the merits unrecognized and the failures blamed with trumps. Thus, efficient accountability in this realm could enhance a better understanding and correction of the intelligence work, as well as it can help to legitimize intelligence policies before the rest of society (not only to intelligence consumers such as policymakers). In light of that, initiatives between academia and intelligence practitioners are more than welcome in terms of fostering an organic relationship to promote historical, theoretical, and empirical studies.[5]

[5] Universidad Rey Juan Carlos in Madrid established a National Intelligence Centre and, in 2005, a Chair of Intelligence Services and Democratic Systems and the following year an Institute of Intelligence for Security and Defence was set up at Universidad Carlos III de Madrid . These initiatives are sponsored as part of a broader 'intelligence culture' project by the Spanish intelligence service: Centro Nacional de Inteligencia (CNI). 2009-10 saw the first cohort of thirty graduates on the MA in Intelligence Analysis taught by the two universities. Inteligencia y seguridad: Revista de análisis y prospectiva, first appeared in 2006 and is now succeeded by the Journal in Intelligence, Security, and Public Affairs (Gill & Phythian, 2016, p. 12).

Epilogue

So far, we have discussed key elements of what is intelligence and the fields of intelligence studies. The evolution of these fields is represented in the following table. From the early constitution of strategic services in the last century, intelligence was conceived as a privileged space of power and decision making for the sake of national security. Nowadays, it can be said that intelligence definition has passed from an aspiring discipline to an interdisciplinary area of studies, incorporating professionals and knowledge from different domains. The focus still relies on strategic national security, but now the scope is also wider and includes even human security dimensions. Of course, state issues have priority, especially if we speak of strategic intelligence at the country level. Yet, human security demands and safety of the population are also essential. Besides, if during the years of Sherman Kent there was a concern in developing theories for intelligence analysis, nowadays we can speak about theories of intelligence that suit different objects and approaches (counterintelligence, financial intelligence, human intelligence, foreign intelligence, etc.).

Table 6: Intelligence studies

The Evolution of the Study of Intelligence		
	Early	**Contemporary**
Definition	Aspiring discipline	Naturally interdisciplinary
Focus	*Narrow*: strategic national intelligence	*Broad*: security intelligence including 'human'
Conceptual concerns	Theories *for* intelligence	Theories *of* intelligence
Key questions	How to improve analysis The analyst-policymaker relationship How to avoid intelligence failure	Relationship between intelligence, state and individual Oversight and accountability Causes of intelligence failure
Area focus	US/UK intelligence	International/comparative intelligence
Level of analysis	National	Multi-level: organisational, national, regional, international
Primary audience	National security practitioners, especially US	Practitioners, policy makers, researchers, scholars, students, concerned citizens

Source: (Gill & Phythian, 2016, p. 18).

Intelligence studies can also be inserted in a shift from a regional focus that emanated from the Anglo-Saxon world to international/comparative studies that

have emerged after the Cold War era, and this work can be understood in that context. Yet, if the level of analysis in this work attaches to the national scale, it is worthy of remembering that intelligence studies can also examine multi-level scales, from regional and international arenas to local and private organizations. In this shift, national intelligence practitioners are still a key audience. However, the intelligence community has been expanded to different audiences beyond policymakers, such as researchers, scholars, students, and concerned citizens. In addition, key aspects related to the intelligence cycle have shifted from a pure vertical dimension (between policymaker that consumes the intelligence product and the analyst) to a wider network between state, intelligence professionals, and overall people. In that sense, oversight and accountability principles are as important as in any other organization and they must be promoted even in scenarios of uncertainty and security risks.

If oversight and accountability have emerged in contemporary intelligence studies, especially since the end of the Cold War, an important connection still must be done between intelligence and surveillance studies. Even if intelligence services, and their former information services to protect the state, can be easily understood as examples of official surveillance deployed against the threats of the state, the nexus between both fields of study has not been fully addressed either by intelligence or surveillance researchers. Epistemologically, in a first approach, intelligence studies can be interpreted as a synecdoche of the surveillance world, a part of the "whole", a part where exceptionality and governmentality trends converge to administrate and regulate the distribution of power in a sociopolitical order. In a second approach, both fields maintain a dialectic relationship that has not been fully explored, especially if we consider the digitalization and the informational aspects of surveillance nowadays.

In light of this, by using examples from the evolution of the intelligence community in Spain and Brazil, we will examine how this field can be connected to surveillance studies. First, we will dig into the past, looking to the legacies of authoritarian regimes over the constitution of intelligence agencies in both countries. The legacies and evolution of those agencies, then, will be essential to assess the accountability mechanisms that have emerged to oversee this realm in the last decades.

3.2. Authoritarian legacies

Bastard, you won't be forgiven
And no, we won't lay down
Tyrant, you're the plague of existence
Tyrant, you're the king of the damned.

Black Mountain, Tyrants, In the Future (Album), 2008.

In the examination of the study cases, it is essential to consider the legacy of authoritarian periods that started after the death of Francisco Franco in 1975 in Spain and after the "aperture" process initiated in 1976 by the Military Joint in Brazil. We consider that past societies matter and are complex in their historicity, refusing the common explanation that the present time is a priori more complex than previous periods. Therefore, we adopt a historical approach for analyzing the past since it can help us to rewrite and understand surveillance nowadays.

The legacy of previous experiences constrains the possibilities of the future. Legacy constraints suggest a theoretical framework stemmed from studies such as critical junctures, path dependence, and new institutionalism. The legacy constraints refer to historical discontinuities and small revolutionary changes that are influenced but still reproduce past institutions and practices. For instance, they are related to critical junctures, a period of significant changes occurring in different ways and places that are hypothesized to produce distinct outcomes if not considered as an explanation (Collier & Collier, 1991). At the same time, this concept is intertwined with other logics, such as the path-dependence theory (David, 2007) which asserts that social outcomes are difficult to modify due to previous policies. In short, legacy constraints emphasize the impact and dependency on previous conditions and practices, either by historical events or political decisions.

Moreover, legacy constraints do not imply that previous politics and values are intrinsically worse than new ones. It implies a political dependency that affects and is reproduced from the past until the present time. That is, the paths opened by the origins are essential. In the sense of historical institutionalism studies (Pierson & Skocpol, 2002) (Immergut, 2006) (Steinmo, 2008), legacy constraints express institutional inertia that marks the trajectory and development of political arenas. Therefore, previous organizations and legal configurations affect certain issues, especially in the case of security. Yet, no single model of change or the impact of past events can do justice to the multiple levels of causality at work in historical explanations. Instead, general units of analysis (such as institutions, laws, and practices) can be used to pose questions and find answers regarding a particular

case or phenomenon (Immergut, 2006). Thus, intelligence institutions and activities are worthy of consideration in order to analyze influences, reactions, cooperation, and conflicts to assess the accountability of institutions that had a remarkable role in the political life of Spain and Brazil. To assess accountability and avoid anachronisms, the intelligence practices will be analyzed within the "spirit" and pace of the historical developments that redefined the political transition in Spain and Brazil. We now address the authoritarian legacy in both countries.

3.2.a. The Spanish authoritarian legacy.

...si la madre España cae -digo, es un decir-
salid, niños del mundo; id a buscarla!...
César Vallejo, 1938.

The Spanish authoritarian legacy inherited by the intelligence services emerged from the ashes of the Civil War (1936-1939), and from the instauration of a dictatorship that lasted from 1939 to 1977. During this period, Generalíssimo or The Caudillo, Francisco Franco, ruled Spain with an iron fist. In 1936, Franco and his forces raised against the Second Spanish Republic in a military campaign that started in Morocco and ended with the final conquest of the major cities including Bilbao, Valencia, Barcelona, and Madrid. With the support of Mussolini and Hitler troops and aviation, the Francoist took over the country and established a dictatorship to erase the Republic and the "communist menace" against the country. The regime was initially isolated from the international community, especially after the Allied victory over the Italian and German dictators in World War II. This isolation led to a scenario of crisis that was reverted since the 1959 "Stabilization Plan" to control economic inflation. Most of the repression and the majority of victims were provoked in the initial twenty years of the regime, a time of austerity in which most of the people lived in rural areas and were illiterate. During the second part of the regime, the nationalist and Catholic ideologies were gradually shifting into a more liberal economic approach, causing the "Spanish economic miracle", and the insertion of the country in the international arena. In the 60s and early 70s, the industrialization and economic development improved significantly, although unequally, the conditions of living. Those years also contemplated the expansion of the incipient middle class. Yet, civic and political rights did not increase in the same rhythm. The mobilization and opposition to the dictatorship by workers and students increased at the end of the regime, although they were present during the whole period (Payne, 2011). In 1969, King Juan Carlos de Borbón was appointed as a successor by Franco to assume the Head of State and the title of Prince of Spain. Franco died in 1975 and the king swore to abide by the principles of the National Movement to perpetuate the regime.

However, a Political Reform Act was passed in a referendum, initiating the so-called transition to democracy in 1977.

Considering the authoritarian practices of the regime, the Francoist installed many concentration camps between 1936 and 1947. The camps, coordinated by the so-called Service of the Military Penitentiary Colonies (SCPM), were an instrument of Franco's repression. The people that ended up in these camps were mainly republican fighters of the Popular Army, combatants from the Air Force and the Navy, political dissidents, homosexuals, gypsies, and common prisoners. During the war, the camps were justified by the fact that "The Caudillo came here [to the conquered areas] in a triumphal march to defeat, not to convince the enemies of Spain" (Benet, 1979, p. 290). Yet, sometimes the Caudillo forces used those camps to convert them to the victorious side of the war.

> Franco was clear that those who survived the camps should leave those places as "reformed men". The prisoners of San Marcos, in León, received a little book in which they were indoctrinated on religion, politics and moral concepts. On these books, they were told: "We hope that some of you leave this place (...) spiritually and patriotically changed; others, with these feelings revived, and all, seeing that we have taken care and taught goodness and the truth". […] In most of the camps, there were also two daily lectures on indoctrination and topics with eloquent titles: Errors of Marxism, Rampant criminality before July 18, The goals of Judaism, Freemasonry and Marxism, Why the Army tries to save the homeland, The concept of imperial Spain […]."[6]

The forms to inculcate "goodness" and the "truth", as expressed in the quotation, remind that disgusting politics can be disguised or covered by layers of "beauty" even in exceptional circumstances. The Caudillo forces interpreted themselves as saviors of the Spanish History and implemented "goodness" and "truth" by a process of dehumanization. The captives were stripped of their belongings and dignity as individuals and social beings. If those actions were interpreted as extreme measures to reach an ulterior goal, the pacification, and salvation of Spain, this utilitarian logic incorporated disgusting methods that were refractory to ulterior beautiful ends.

To recreate a new country and "correct" the enemies, the Spanish camps were not organized as the Nazi camps during the "Final Solution" in World War II. Franco forces improvised most of the camps during the campaign against the Republic. However, the initial repression of the Caudillo provoked the diaspora of thousands of civilians to other nations. During the Spanish Civil War from 1936 to 1939 and in the first years of the regime, a considerable part of the population was forced to move to other countries, for political and ideological reasons, or due to

[6] De Miguel, C. H. 2019, March 19. 'Terror en los campos de Franco'. *El País, semanal.* Retrieved from: https://elpais.com/elpais/2019/03/04/eps/1551726594_395569.html

fear of reprisals by the winning side of the quarrel. Those people remained abroad until the pacification of the country, although many of them stayed abroad and lived in foreign countries.[7]

There is no aim to depict an exhaustive analysis regarding the Franco repression. However, one paradigmatic example of the authoritarian legacy and surveillance from those years comes from the repression executed against teachers. Some historians do not hesitate to mention that teachers suffered most of the repression because "They were responsible for injecting the Republican virus to the general society and especially to young people" (Valero, 1997, p. 94). After the victory in the Civil War, the regime focused on this group to inflict exemplary punishment to the so-called illustrated people and intellectuals. Those who survived the military uprising experienced an internal exile due to the purges and the pedagogical reforms implemented by the government. Besides, fear and silence were common in schools and teachers' families. Valero (1997) has identified up to 60,000 "reformulated" teachers in his book "The Debugging of the National Magisterium" (free translation). Other scholars like Morente explain that not only the "purification" came from above, but it also consisted of mutual surveillance among neighbors and friends. "There were private complaints, from neighbors, in which a teacher was accused of playing the piano in public, for example". In a town in Lugo, the mayor fired an old teacher because in his place it would be better to have a "Catholic lady from a decent family, as God commands."[8] The educational purge expelled nearly 15,000 teachers and sanctioned about 6,000. Even university professors did not escape from the purge that stripped many of their works as they were replaced by people who were aligned to the regime.[9]

Because of the Civil War, the silence imposed over the victims, and the following repression, it is impossible to determine the exact number of victims and missing persons. Yet, some studies mention between 150,000 and 400,000 dead depending on the time and the inclusion of victims killed in concentration camps (Vilar & Gázquez, 1986). Regarding the prisoners in Francoist concentration camps, 192,000 would have been shot, including those executed after the war (Vilar & Gázquez, 1986). In the postwar period, during the regime, surveillance was deployed to restore the virtues aimed by the government. It was necessary to

[7] It is known that a generation of common people as well as of intellectuals left the country due to the Civil War and the subsequent repression. For example, the physicist Blas Cabrera, the writers Tomás Segovia, Emilio Prados, Max Aub and José Bergamín went to Mexico. The doctor and biologist Severo Ochoa, the philologists Américo Castro and Tomás Navarro Tomás, the writer Ramón J. Sender, the professor and politician Fernando de los Ríos and the family of Federico García Lorca (his father, his brother Francisco García Lorca, his sister Isabel García Lorca) to the United States, while the writer Manuel Altolaguirre went to Cuba. The Generation of 27 was dispersed throughout Europe and the Americas (Glondys, 2012).

[8] De Miguel, op. cit.

[9] In extreme cases, the regime ordered the execution of the rector of Oviedo, son of Leopoldo Alas, and of the rector of Granada, favorite disciple of Unamuno, as cases of exemplary punishment (Claret Miranda, 2006).

create “Irreproachable people from the religious, ethical and national point of view.”[10] Thus, it is important to mention several surveillance mechanisms and repression measures beyond physical violence. For example, in labor, citizens needed to show their alignment to the regime to obtain a job or to receive social benefits. Otherwise,

> Officials were punished with sanctions ranging from incarceration, forced transfer, suspension of employment and salary, disqualification and separation. To obtain a job, priority was given to those loyal to the National Movement, or to people who presented “certificates of good conduct” issued by the local head of FET and the JONS - through the reports of the Information and Research Service – with the approval of the local Church priest […]. In addition, employers' organizations made lists of “reds” and “trade unionists” to prevent them from entering in companies. In the case of liberal professionals, a sort of control over their work was implemented by their associations, and, in the case of Public officials who served during the Republic, they were dismissed in accordance with the “Law of Purification” (Casanova, Fontana, & Villares, 2007, p. 112).

As parallel mechanisms of surveillance, political parties, unions, associations, and newspapers not related to the regime were banned. Freedom of expression against the government or the simply disagreements was annulled, and a system of censorship of all media was established by the same instances of government. Censorship started to be common to monitor literature, poetry, music, plastic arts, film, and theater. A defined cultural model was imposed according to the criteria established by the state. The censorship affected every intellectual activity and the media, and even included photographic manipulation. For example, before being represented, plays needed to pass the filter of the “Board of Censorship of Theatrical Works” that, in many cases, imposed the elimination of phrases, distortion of dialogues, and even their total prohibition (Neuschäfer, 1994). The incipient realist theater, influenced by novels and the realist cinema, was forbidden because it was considered a “school” of Marxism (Muñoz Cáliz, 2005). Moreover, works that represented aspects of the Spanish reality that the regime was trying to hide were also censored. Freedom of expression was only recovered on March 4, 1978, during the democratic transition, when the Royal Decree 262/1978 abolished the censorship to perform theatrical activities in the country.

In the 1960s, one of the most relevant phenomenon in terms of violence and social responses against the regime involved national separatists such as the Basque ETA. Born from a youth sector from the Basque Nationalist Party that thrilled a more establishment path, the dissident youth movement embraced radical contestation as a form to expel what they considered “forces of occupation”

[10] De Miguel, op. cit.

and “colonialists” sent by the Franco administration and the French government to rule the regions deemed as historical lands by the Basques (Tusell, Alted, & Mateos, 1990). In that strategy of “indigenous against invaders” inserted in a bigger movement of decolonization of the world, the group also embraced Marxism promoted by the growing labor conflict in industrialized zones. ETA actions ended up conditioning the Basque socio-political life as the violent actions provoked harsh repression that, frequently, did not only hit ETA and proxy groups. The scale of repression from the centralist administration in historical regions, such as in Basque and Catalonian cities, provoked considerable rejection against separatist groups as well as massive resentment against measures of the central government. For example, the Public Order Tribunal (TOP) was created to “repress crimes that subverted the basic principles of the State or that planted anxiety in the national consciousness” (Law 154/1963), as if the country should have only one way of thinking. The Tribunal only disappeared in 1977, two years after Franco’s death and during the beginning of the Spanish transition that also affected the realm of intelligence. We will return to this point later.

3.2.b. The Brazilian authoritarian legacy

Monument “Tortura Nunca Mais”, Recife.
Photo: André Occestin. Flickr.

In Brazil, the authoritarian legacy that affected intelligence can be traced to the times of the New Republic and the military interventions after the end of the World War II.[11] When the vice-president João Goulart became president of Brazil as Janio Quadros renounced in 1961, deep polarization emerged amidst the Brazilian society. Different groups feared the Cuban influence and the Communist threat. Influential politicians (such as Carlos Lacerda, and Juscelino Kubitschek), media moguls (Roberto Marinho, Octávio Frias, Júlio de Mesquita Filho), the Church, landowners, businessmen, and the middle class requested a coup d'état by the Armed Forces to remove the leftist government. The “hardline” group of the military, having the chance to impose their economic agenda, convinced the loyalist groups to overthrow Goulart and the communist menace. The Coup D’état happened on April 1 of 1964. Due to the declassification of official documents, historians nowadays interpret the removal of the president Goulart as a clear

[11] In this period, the military played a key role guiding the political life of this country through coup attempts and military interventions. This role is even older and dates to the Paraguayan War (1861-1865), the Proclamation of the Republic, which overthrew the Empire (1889), and the Revolution of 1930 (De Carvalho, 2019).

intervention influenced by the United States to restrain communism in the biggest country of Latin America.[12]

Due to the military intervention, Congress elected the Army Chief of Staff, Marshal Castelo Branco as the new president. Castelo Branco and the follower presidents ruled the country by "Institutional Acts" ("Ato Institucional" or "AI"), from which the executive obtained the ability to change the Constitution, remove anyone from office ("AI-1") as well as to have the presidency elected by the Congress. A two-party system was created as a solution to monitor dissidents and control politicians. In that system, candidates only could run through the government party –the National Renewal Alliance (ARENA)-, or the controlled party opposition –the Brazilian Democratic Movement (MDB) ("AI-2").

General Artur da Costa e Silva followed Castelo Branco as a president who represented the hardline group from the military. In 1968, Costa e Silva signed the Fifth Institutional Act ("AI-5") that enacted dictatorial powers, the Executive dissolved the Congress and state legislatures, suspending the Constitution, and imposing censorship. The next president, Emilio Garrastazu Médici, was also a hardline general that sponsored human rights abuses. During his government, persecution, and torture of dissidents, harassment against journalists and press censorship became ubiquitous. The anti-government manifestations and the guerrilla movements were targeted by the increasing repression of the regime. Urban guerrillas, such as Ação Libertadora Nacional and the Movement 'October 8', were fiercely suppressed. In addition, military operations vanquished the Araguaia guerrilla in the backlands of the country. Meanwhile, the government promoted the economic boom acknowledged as the "Brazilian miracle" due to industrialization policies, nationalist programs, and commodities exportation (De Carvalho, 2019).

In 1973, the electoral council controlled by the Armed Forces elected General Ernesto Geisel as the president of the country. In 1974, Geisel purged regional commanders by trusted officers and labeled his political program as "abertura" (opening) and "distensão" (decompression). This year represented the starting point of the gradual distension of the authoritarian rule. Alongside the minister Golbery do Couto e Silva, the president announced his slow democratization plan despite the threats and opposition from hardline military groups. In that context, the torture of dissidents was rampant as exemplified by the murder of the journalist Vladimir Herzog. In 1977, when the opposition MDB party won more seats in the House of Deputies, Geisel convoked again the AI-5 to dismiss

[12] In an operation called Operation Brother Sam, The USA positioned war ships in the coast of Rio de Janeiro in case Brazilian troops required military assistance during the 1964 coup. A document from Gordon in 1963 to US president John F. Kennedy also describes the ways João Goulart should be put down, and his fears of a communist intervention supported by the Soviets or by Cuba (Fico, 2008).

the Congress. In that year, he also enacted a series of Acts for indirect elections in states and regions.

In the next years, Geisel allowed exiled citizens to return to the country, restoring habeas corpus, and abolishing the AI-5 in 1978. In turn, he imposed General João Figueiredo as his successor in 1979. Figueiredo, an Army General and former head of the secret service (the National Intelligence Service of Brazil), steered the country back to democracy in a context of a severe economic crisis and promoted the devolution of power to civilians. Despite the opposition from hardliners, Figueiredo continued the gradual "abertura" (opening) process. In 1979, the Amnesty Act absolved people convicted by "political" crimes since 1961. In addition, due to increasing opposition to the regime, the two-party system was abolished that year.

In 1981, the National Congress reestablished direct elections for state governors and, two years later, mass popular movements claimed direct vote to elect the next president ("Diretas Já") symbolizing the re-establishment of freedom of assembly and freedom of expression. However, the popular claims were ignored and, in 1985, the Electoral Council indirectly elected the first civilian president. In this election, the opposition candidate Tancredo Neves succeeded Figueiredo. Yet, due to Neves's health problems and his death, vice-president José Sarney commanded the country until 1989. Because of the gradual process of distention towards a new Republic, it can be said that the Brazilian transition, like the Spanish one, was arranged and gradually controlled by the military and civilian elites.

Considering the authoritarian practices of that period, the Brazilian military regime provided a model to other dictatorships in Latin America. This country systematized the "National Security Doctrine", which "justified" military intervention to preserve the national security in times of crisis. The Doctrine enacted the intellectual base and the repression methods shared with other military regimes (Borges, 2003). In 2014, nearly 30 years after the end of the regime, the Brazilian military recognized for the first time the excesses committed during the years of the dictatorship, including torture and murder of political dissidents.[13] It is calculated that 434 people were either killed or became missing persons during the dictatorship. Although human rights activists rise this number, the Armed Forces have always contested those statistics.

> While other dictatorships killed more people, Brazil saw the widespread use of torture […] Advisors from the United States and United Kingdom trained Brazilian forces in interrogation and torture. To supress

[13] In May 2018, the United States government released a memorandum, written by Henry Kissinger (who was Secretary of State at that time), dating back to April 1974, confirming that Geisel was fully aware of the killing of dissidents. See: Borges, R. 2018, May 18th. 'Documento da CIA relata que cúpula do Governo militar brasileiro autorizou execuções'. *El País Brasil*. Retrieved from: https://brasil.elpais.com/brasil/2018/05/10/politica/1525976675_975787.html in 03/10/2019

> opponents, the dictatorship used arbitrary arrests, imprisonment without trials, kidnapping, and most of all, torture, which included rape and castration. [...] French General Paul Aussaresses, a veteran of the Algerian War, went to Brazil in 1973. General Aussaresses used "counter-revolutionary warfare" methods during the Battle of Algiers, including the systemic use of torture, executions and death flights. He later trained U.S. officers and taught military courses for the Brazilian military intelligence (Oliveira, 2011, pp. 19-20).

Between 1968 and 1978, under the AI-5 and the National Security Act of 1969, the so-called Years of Lead (Anos de Chumbo) were characterized by a state of permanent exception. From that year, the military strived to the last consequences in their fight against the armed resistance in Brazil. According to the Brazilian Army Commission in Washington (CEEW), death squads prosecuted and killed communists and other dissidents in the domestic land and abroad. As in the case of the Spanish Civil War, the Brazilian military believed that their measures were part of an exceptional time that demanded tough answers against a stealthy enemy. For example, when Carlos Lamarca left the army to create a leftist guerrilla called MR-8, the military captured Lamarca allies such as Stuart Angel Jones. Army and navy officials tortured Jones to dismantle the MR-8 organization and its leaders. As in a Kafkian dream, the destiny of Jones after his detention is still unclear. According to some witnesses from the military, he was tortured to death by disgusting methods that we will not mention because of its horribleness. Nevertheless, the official version of the military refused his murder and considered Jones as a missing person. Zuzu Angel, Jone's mother and USA citizen, denounced this case to the Brazilian and USA diplomatic embassies. She also denounced the case in the media, writing letters to politicians, and giving interviews with investigative commissions (Simili, 2014). Yet, no truth was discovered about the fate of Jones. Zuzu died in a car accident in Rio de Janeiro in 1976. The mortal remains of the student, as well as from other dissidents, never were found.[14]

In the cultural field, music, plays, movies, and books were censored by the regime. The press that criticized the government or revealed alternative ideologies was not allowed. Because of the daily censorship, some newspapers such as "O Estado de São Paulo" decided to use their pages to publish cuisine receipts or excerpts from "The Lusiads", by Luís de Camões, a classic Portuguese writer from

[14] The story of Olavio Hansen is also similar to dozens of other cases in the period. He was arrested during an act of the Labor Day on May 1, 1970 in Vila Maria, north of São Paulo, and died at the Military Hospital of the 2nd Region in Cambuci. He did not resist a week of torture at the State Department of Political and Social Order of São Paulo, which included hours on the Pau de Arara, shocks, burns with cigarettes and the dragon's chair. In the necropsy report, several bruises were noted - including the head. In some of these torture sessions the shocks were applied with such intensity that left burns on the chest near the heart, which were also reported in the postmortem report. In an attempt to cover the crime, official authorities said that Hansen committed suicide (Kucinski & Tronca, 2013).

the 16th century.[15] In 1968, members of the extreme right-wing "Communist Hunt Command" (CCC) invaded the Ruth Escobar Theater in São Paulo and battered the cast of "Roda Viva", an acknowledged drama group at that time. The police collected pieces of evidence without investigating the crime. Either through direct pressure or omission, the dictatorship ended up stifling the national culture as many artists were surveilled by their "attempt to break the law or by subverting the "Brazilian Democratic State established in the Revolution of 1964" (Simili, 2014, p. 37). In addition, Brazilian public universities lived under heavy surveillance: teachers were compulsorily retired, students expelled, and books censored. The censorship, carried out by the "National Telecommunications Council" (CONTEL), an organization under command of the National Information System (SNI), prohibited the exhibition of films, photos, radio, television broadcasts, as well as collective manifestations of students. To complement this scenario, bookstores, libraries, and houses of intellectuals were randomly "visited" by security officials at any time.[16]

In the international arena, in 1975, the Brazilian regime was secretly allied to similar dictatorships such as the Chilean, Argentinian, Paraguayan and Uruguayan regimes. Those countries worked together to the implementation of *Operation Condor*. This consisted of a secret plan for the suppression and extermination of political dissidents from those regimes in South America, North America, and Europe. Even if the results cannot be attributed solely to that operation, they are astonishing. There were at least 85.000 dead or missing, 400.000 tortured, and more than 1000 foreigners expelled from the above countries. The Brazilian military regime was considered the leader country of the Operation (De Souza, 2011).

Epilogue

So far, we have mentioned the previous political context that marked the dictatorships in both countries, as in the case of the Civil War in Spain and the instability of the New Republic in Brazil. In terms of institutional leadership, the Spanish Case is remarkably known by the centralization and unipersonal rule of Francisco Franco, especially when compared with the Brazilian model that consisted of a succession of indirect military Presidents elected by the congress or by a Joint Council. We also mentioned some examples of repression by hard means such as concentration camps, summary executions, and torture in Spain; and

[15] Mayrink, J. M. 'Acervo mostra as marcas da censura'. *O Estadao*. Retrieved from: https://economia.estadao.com.br/noticias/geral,acervo-mostra-as-marcas-de-censura,113609e in 07/10/2019

[16] On August 30, the Federal University of Minas was closed and the University of Brasília invaded by the police. AI-5 increased censorship and control of Brazilian society. As a direct consequence of the Act, journalists and politicians, professors and students that were suspect of be against the regime were removed from their positions and in some cases arrested by the security forces (Motta, 2014).

torture, forced missing, and death squads in Brazil. In both countries, the regimes also deployed "soft" means of repression such as censorship and continuous surveillance that facilitated the vigilance among regular citizens (like neighborhoods, families, factories). Yet, official surveillance was exercised especially over politics and public administration, as well as in education, labor, religion, culture, and arts. Besides, it could be said that the nature of the transition, after the distention of the regimes, consisted of arranged processes established by the military and civilian elites. This allows us to establish a social and historical similarity between our cases as summarized in the table below.

As Table 7 shows, in terms of victims and missing persons, the numbers are very disproportional between both countries. This is because a considerable proportion in the Spanish case comes from the campaigns and repression after the Civil War. The conflict caused demographic regression and a wave of Spanish refugees left the country. In Brazil, compared to other authoritarian experiences in Latina America and Europe, it has been said that the dictatorship was more "efficient" to execute repression of dissidents and political foes, producing a smaller amount of casualties. Perhaps, this "efficiency" should be circumscribed to the expertise of security forces and the counter-insurgence and intelligence capabilities acquired from international collaborators, as well as to the development of the "National Security Doctrine". However, the fact that this country has less victims needs to be contrasted with the dark cipher of cases and the impunity to assess crimes. Besides, rampant torture and fear are hard to be measured. Moreover, in both cases, the fact that official institutions and governments used abject methods to implement policies must not be placed at the same level of the violence produced by resistance and counter-insurgent groups, even when violence in the two sides is deplorable.

Table 7: Authoritarian legacies in Spain and Brazil

	Spain	Brazil
Previous context	Civil War ending the Second Republic (1936 -1939)	Instability from the New Republic (1945 – 1964)
Authoritarian regime	Francisco Franco dictatorship (1939 – 1977)	Military dictatorship (1964 – 1984)
Institutional leadership	Centralized and unipersonal model	The succession of military presidents elected indirectly by a Joint Council
Distention process	Franco`s death in 1975.	Opening process initiated by the general Geisel in 1974.
Main forms of repression	Suspension of political and civil rights • Hard repression (concentration camps, summary executions, torture) especially during the civil war and at the end of the regime. • Other measures (purges, censorship, etc.) during the entire regime.	Suspension of political and civil rights. • Hard repression (rampant torture, forced missing, death squads) especially after the AI-5 of 1968. • Other measures (purges, censorship, etc.) almost during the entire regime.
Main areas of surveillance	• Politics and public administration • Education	• Politics and public administration • Education

	• Labor and religion • Culture and arts	• Labor and religion • Culture and arts
Authoritarian Legacy	• Between 120 000 and 400 000 death and missing (Vilar & Gázquez, 1986). Half of them during the Civil war campaign. Thousands of refugees and exiles. • Amnesty law passed in 1977 • Judicial reluctance to process the crimes of the dictatorship • Antagonist memory, cosmopolitan memories, agonistic grounded memory, and the problem of forgetfulness • Law 52/2007 to initiate historical reparation of victims	• Between 400-500 death or missing. Around 1000 tortured and 1000 exiled. • Amnesty Law passed in 1979. • Judicial reluctance to process the crimes of the dictatorship • Antagonist memory, cosmopolitan memories, agonistic grounded memory, and the problem of forgetfulness
Type of transition	• Arranged between the military and civilian elites. • Pressure from bottom groups to enact a political reform and a Constitution in 1978. • Pressure from bottom groups to achieve more historical autonomy (i.e. Basques and Catalans).	• Arranged between military and civilian elites. • Pressure from bottom groups to reach direct Presidential elections in 1985 (negated). • Pressure from bottom groups to enact a Constitution in 1988.

Source: the author

Here the historiographic debate is open between those who put a proportional amount of responsibility regarding the level of violence and the number of victims produced by each side of the quarrel -between government repression and the subversion. Yet, we believe that even when the violence and abject methods were used in a context of conflict and turbulent years; it does not excuse insurgent groups and official institutions from their responsibility, especially when this side had more resources, inflicted broader surveillance over their populations, and continued to rule the countries. That is, the asymmetry of power between the regime and its rivals, during a considerable part of the Franco and Brazilian dictatorships, was not equilibrated, and pended in favor of the official institutions (especially if we think security and surveillance measures deployed on political and cultural fields).

Finally, even if we think in a third via in which the violent methods of the governments were justified to contain a violent opposition, the official institutions should be scrutinized by the authoritarian legacy that they promoted and by the emergence of new collective memories to deal with violent past actions. Even when the number of victims does not compare to other dictatorships, counting the victims or the missing persons from those times cannot be measured and retold with accuracy in human terms. Thus, the "small" amount of victims also matters. Surveillance and fear consist of the internalization of disciplinary routines and a dialogic relationship between individuals and communities. In that sense, the

mortal remains and the common fosses to be unearthed are just tips of the iceberg in a form of repression that was exercised also by soft means and by the normalization of exceptional measures for the sake of security and the country.

In terms of collective memories, relative progress has been done since the end of both dictatorships. After the Amnesty Act passed in 1977 and 1979 in Spain and Brazil respectively, the legislation tried to put aside from justice the violent practices of the regimes, avoiding revenge and turmoil in the distention process started after the death of Franco and the Brazilian distention ("abertura"). That is, avoiding legal complaints and political rivalries were considered as a necessary truce to promote peace and establish a base for a democratic transition. However, this effort was failed in terms of a peaceful transition, since the cycle of violence between the dissidence and the government expanded as in the case of terrorism and counter-terrorism killings committed in Spain after 1977. If Amnesty was necessary, at the same time, it was an incomplete exercise of political transition that nowadays in seen with skepticism. Especially because the transition was never complemented by the official "mea culpa" and by the reformulation of consistent remembrance policies in both countries, especially within the military institutions. Military doctrines might still interpret past interventions in a utilitarian perspective that promotes the archetype of "saviors", an aggressive position that was necessary to defeat a menace and defend the country.

The memories of this period are still alive and the ashes of the repression are still warm. During the last decades, the intervention on common graves and other expressions such as war museums, as well as theoretical and practical works on historical memory have counteracted the mere antagonistic political debate in this issue, as well as the messianic memory of the military. That is, the historical exercise has dissipated some myths that exacerbated ultranationalist feelings of heroes and demons without nuances. This memory is what theorists call "the most basic antagonism", which became secondary after the Cold War since 1989. After this year, analytical and administrative models have arisen from the reflections on the Holocaust. Those reflections are based on human rights and principles of truth, justice, reparation, and the guarantee of non-repetition, with the victims at the center of the collective memory. In the case of Brazil, this was the approach of the "Truth Commission" organized by civil society from 2011 to 2014, but this work has not been accepted by the military. Despite this kind of commissions, legislative reforms and international cooperation, many battles over collective memory persist. At the same time, forgetting the terrible and disgusting past of these countries emerged as a problem of forgetfulness, a sort of collective amnesia that turns every historical and ethical effort extremely difficult. This problem might also emerge alongside new forms of authoritarianism, promoting the return of primary dichotomies between heroes and demons as seen in the last years.

To avoid the consolidation of the authoritarian return, while some scholars say that we need to finally make peace with our violent past, by building social, cultural and pedagogical spaces where critical analysis are possible; other groups say that we need to face our violent past in a more sincere way (Beverley, 2011). In the latter vision, the cosmopolitan model consist of the agglutination of several and heterogeneous memories. Yet, this model might depoliticize the classic terms to process memory and equalize the collective memories with the collection of archives and testimonies to be stored in a 'sterile museum'. Thus, linking a cosmopolitan memory with a sincere political discussion is an imperative model nowadays. Some experts have called this point of convergence as the "agonistic" path or model (Pérez, 2013). This path consists of increasing the democratic quality of discussion so that different memories can coexist, but always within a basic ground where people respect the cognitive and deliberative limits of this environment –like respecting victims and not supporting violent methods anymore. Notwithstanding, this convergence is not the harmonization of discourses and the definitive resolution of historical conflicts. After five decades of transition in both countries, the pressure to obtain a basic ground to collective memories still clashes against institutional and legal dimensions. Some examples are the long judicial process until 2017 for the exhumation of 50 people shot during the Civil War in Guadalajara, Spain[17]; another example is the failed request in 2015 of the Truth Commission to the military to assume their role during the implementation of torture during the Brazilian dictatorship (Pereira, 2015). That is, despite the intense debates historical memory provokes in Spain and Brazil, there are both actions and discourses of conscious forgetfulness that prefer to see the ashes of the past extinguished. In this vision, the memory should remain in the past. Yet, this trend ignores that even forgetting is a political act, and as forgetfulness is used to avoid the corrosion of the arranged transition, especially in Spain, or to ignore the victims of the regime, as in the case of Brazil, those actions maintain the ashes of the past even warmer and alive.

In the summer of 2020, the mortal remains of 1,103 people started to be unearthed in the Pico Reja mass grave in Seville. Historians place this grave as one of the largest in the country. The first murders in Seville happened in this location after the uprising in 1936, including the execution of Andalusian intellectuals, such as Blas Infante, the mayor of the city, Horacio Hermoso, as well as other politicians and town councilors. Two kilometers away from this grave, the mortal remains of the Francoist General Queipo de Llano, responsible for the execution of 50,000 people, are buried in the Macarena Cathedral. The asymmetry of power is reflected even in the position in which the mortal remains are buried and rest. That same year, the Spanish government ruled a bill of Historical Memory to exhume Franco's

[17] Aunión, J. A. 2019, March 11th, Europa busca se reconciliar com seu violento século XX, *El País*. Retrieved from: https://brasil.elpais.com/brasil/2019/03/10/cultura/1552238060_048323.html in 03/13/2019

graveyard and to update Law 52/2007. If approved, the state will assume more responsibilities to help social organizations to find missing bodies and to guarantee civil protection to victims of the dictatorship.

On the contrary, Brazilian attempts of historical justice have failed in the last years. For example, over a thousand people from the dictatorship still await forensic identification in the clandestine *Vala de Perus* graveyard, unearthed in São Paulo 30 years ago. From 1,049 people dumped in the ditch, about 42 were political dissidents. Also, two thirds of the bones might belong to children and teenagers as these groups were the major victims of the 1970s meningitis epidemic that hospitals were unable to treat during the dictatorship. Even in this site, the state role to recognize and identify people is daunting. In other domain, in in prisons, living people are left to die or considered as bare life. Decree 9.831/2019 abolished the non-governmental committee that monitors the use of torture in the prison system. According to the Brazilian government, it was necessary to abolish public institutions influenced by groups influenced by NGOs and universities. This action corrodes the fragile national policy to combat torture in a country that has the third-largest imprisoned population in the world (around 720,000 prisoners) and a vast history of abuses by state institutions. The Decree shows that lessons from the past are hard to be learned. Furthermore, it shows that the ashes of the past can light dangerous and authoritarian fires that seemed to be extinguished.

3.3. Intelligence institutional paths

The specificity of Francoism did not differentiate Spain from Brazil when we assess, in the transition of each country, the role of the military within the intelligence agencies. Indeed, the internal transition of the secret services in both countries resembles similarities. In the internal transition agenda, the superior ranks -predominantly military from the Armed Forces- used their institutional power to reproduce the Lampedusa effect: it was necessary to change in order to preserve. This tendency can be a strong obstacle to political transition, especially to promote the accountability of bureaucracies that emerged from authoritarian regimes.

In the Spanish and Brazilian cases, the characteristics of the old regimes shown in the last section offer clues about the institutional changes of intelligence services. However, it is necessary to look at the intelligence services and evaluate their role in the transition. It is important to trace, therefore, the authoritarian legacies within these institutions. That is, now we explore the institutional designs, the mechanism of surveillance, and the ways used to adapt or resist to the transitions initiated in 1975 in Spain and 1976 in Brazil. Without this endeavor, it would be not possible to identify and assess the mechanisms of accountability created to control those institutions.

3.3.a. The Spanish path: SECED, CESID, CNI

During the Franco regime, the Spanish administration executed policies due to the support of "information departments". In Foreign Affairs, Tourism, Labor, and other ministries, specific departments collected and produced information to supply urgent administrative demands (Peñaranda, 2005). In terms of security, the Ministry of “Gobernación” -later, Ministry of Interior- had two departments supporting security and public order responsibilities: the Information Service of the Civil Guard Police, and the Office of Information -later General Commissariat- integrated to the General Directorate of Security. In the late 60s, the General Inspector Office of the Armed Police also had a small informative department for internal demands.

In the military domain, the Information Service of the Armed Forces -the Third Section of the High Chief of Staff- fulfilled missions vaguely considered as “espionage” both at state level and in foreign countries with the support of international services.[18] This center provided key information of different types for

[18] The Major Chief of Staff was created in 1939 after the Civil War to provide the Supreme Command of the Military the necessary information for the most accurate appreciation of the military and economic potential of other countries. Its Second Section was responsible to surveille

the decision making. The Third Section produced something that in the Anglo-Saxon started to be called as "intelligence". A sort of refined information disseminated to superior ranks, to the Head of the State and the Presidency. The information flow was secret and followed the orders from high-ranked bureaucrats in the Armed Forces (Peñaranda, 2005). Meanwhile, the Third Section validated its channels of information by contrasting internal sources with external informants.

In 1962, the Third Section was updated to execute tasks of counterintelligence, to control communist activities and monitor the links with Russia and Cuba (both in Spain and in foreign soil), to control anti-regime organizations, and to surveille trade unions and universities. Some authors claim that those tasks have not been executed with sufficient staff and resources, resulting in poor performance and efficiency.[19] The lack of efficiency of the military information services became evident when the regime faced increasing opposition, especially by labor unions, clandestine parties, and student movements after May 1968. In these times, neither the military forces nor the information services of the police had the capability and the methods to counteract the political turmoil. In light of that, key people had the initiative to create what would become the strategic office of intelligence in Spain. One of these was Colonel José Ignacio San Martín, who established the "National Countersubversive Organization" (OCN).

In his autobiographical book *Special Service: To the orders of Carrero Blanco*, San Martín (1984) confesses his youthful inclination to espionage issues and cryptography. He also mentions that the regime was concerned about the radicalization of students at universities. According to him, superior ranks of the government wanted to avoid the turmoil that affected France and other European countries after the cultural youth revolution in 1968. In order to do so, the hand of Franco, the general Carrero Blanco, authorized the creation of the OCN. In his book, San Martín mentions that he received the following instructions to create the OCN: 1) to support the Minister of the High Chief Staff (AEM) on information matters; 2) to coordinate the departments of the Ministry that had analogous functions (for example, from the Army and the Civil Guard); 3) to not mention or link the AEM with ulterior operations; 4) to obtain information through the capture of informants and the infiltration of agents; 5) To locate the Office outside the AEM facilities; 6) to give documentation and archive support to the AEM's Internal Affairs Bureau; 7) To establish relations with the AEM through the Chief of

political dissidents in France and elaborate periodical briefs about their situation (Zorzo Ferrer, 2005).

[19] According to Zorzo Ferrer (2005), a proof of the mentioned inefficacy is that, in 1966, the Special Service Operations Section was created within the Third Section in order to carry out certain operations. In 1972 the focus of this organization lied on the field of counter-espionage. Once the SECED was established, the tasks assigned to the AEM were related to external intelligence activities, counterintelligence, and espionage of the radio-electric space.

Operations of the Third Section, and 8) to elaborate the Action Plans to be approved by the AEM Third Section (San Martín, 1984).

When the office was settled in Madrid in 1968, San Martin refered to the OCN as an office specialized in the process and dissemination of information received from other services. In his words, the OCN had the following divisions:

> -Department of Documentation, studies, and reports (information processing)
> -Department of research (to develop its own information)
> -Technical support group (for improving the previous tasks) (San Martín, 1984, p. 46).

Since the creation of the OCN, San Martin expressed that the work of the service should not replicate the work conducted by the Armed Police and by the Political-Social Brigade as these institutions had already consolidated channels to gather and process information. Furthermore, as activities related to surveillance, the Office was responsible for

> -Creating an analogic file system of persons who were supporters or adversaries of the regime, as well as a list to examine the so-called groups of "pressure".
> -Studying all clandestine groups and organizations.
> -Creating Sectoral files.
> -Deploying information networks
> -Elaborating special research operations with modern means and techniques for the time (50 operations per year, approximately).
> -Researching technical means and acquiring appropriate material for the services. […]
> -Disseminating information and technical expertise to state agencies
> -Forming addicted movements (supporters of the regime).
> -Deploying psychological actions through the orientation of the public opinion and promoting links with the Cabinet of Psychological Action or GAP (San Martín, 1984, p. 46).

Even if the tasks were not fully deployed, or whether San Martin words are a personal memory to polish his legacy and the Office image, what is true is that the tasks and forms of surveillance mentioned above targeted scholars, trade unions, and religious groups since 1968. In San Martin's words, the OCN tried to “restrain and reduce the subversive process; suppressing insurrection energies”. For him, it was important to “eliminate or reduce the existing problems in the whole society and the Administration; as well as to open channels of participation to foster a political evolution” (San Martín, 1984, p. 31). Again, his words can be interpreted as a clear statement to justify the effort to redefine the future of the

country. The last phrase can be inserted in a clear retrospective attempt to justify the role of the Office in the coming political transition after Franco.

When Francisco Franco died in 1975, the OCN was previously transformed into the "Central Documentation Service" (*Servicio Central de Documentación* - SECED) in 1972. This change was the result of the professionalization and institutionalization of the OCN. In that sense, Díaz-Fernández (2006b) affirms that the good relationship between San Martín and his supervisors, including the Presidents of the government, promoted the SECED into a new level. The Center received more materials, staff, and information. During its first years, SECED personnel worked in every Ministry or Executive Office in Spain. Those members supplied the Center with fresh and valuable information every day. These methods allowed the new governments to spy internal adversaries and to monitor even military groups as some of them wanted to abolish the arrangements of the political transition (Díaz-Fernández, 2006b).

As mentioned, the administration of the Center depended on the harmony between bureaucrats and politicians. In that sense, the appointment of Arias Navarro as President of the government just before the death of Franco resulted in the dismissal of San Martin as Director of the SECED. Juan Valverde, a former Commander of the Infantry and friend of Navarro, replaced San Martin in 1975. Since the death of Franco in 1975 to the Political Reform in 1977 tensions emerged among the military as some wings wanted to influence the political transition. A proof of this is a classified document leaked to the press in September 1977. The document, released by the French journal *Le Monde Diplomatique*, retells a conversation of the high military staff from the General Information Direction attached to the Security Staff of the Ministry of Interior.

> According to news gathered in the town of Jática, a secret meeting between the high military commanders was held yesterday under the presidency of Lieutenant General De Santiago. The group reviewed the current Spanish situation and decided to abide, at this moment, by the legality principles to respect the transition and the King. They also expressed the Army's loyalty, urging the King, in the face of the current serious situation, to replace the Government with a stronger and apolitical figure oriented by the Lieutenant General and by representatives of the three Armed Forces (Le Monde Diplomatique, in Almenara, 2012, p. 155).

The military advice to the King was one example of the tensions that emerged to conduct the transition after the death of Franco. At the time of this event, Adolfo Suarez was the President of the Government since 1976. Although the advice was given, the King ignored the military pressure to replace the President and maintained Suarez. With the king support, Suarez supervised the beginning of the transition, legalizing all the political parties (including the

Communist Party, a particularly difficult decision contested by the hard-lined groups) and won the general elections in 1977. In this year, and following the reforms promoted by Suarez, the **SECED** was also transformed into the **CESID**, "the Superior Center for Information and Defense" (Centro Superior de Información para la Defensa).

When the SECED was transformed into the CESID, Suarez expressed that the surveillance of leaders and legal political parties was not allowed in a democratic regime. Yet, his words did not change previous practices. The CESID still targeted Francoism representatives in the Parliament that were against the Political Reform. In addition, extreme right and leftist groups that initially were outside the transition became targets of interest to the new political regime. Also, eavesdropping and interception of foreign embassies in Spain was prohibited. In practice, however, the prohibition was not fully implemented (Díaz-Fernández, 2005).

The creation of the CESID is also explained because the political transition demanded a new role for security institutions. In that logic, the Ministry of Defense, Manuel Gutiérrez Mellado, replaced the information agencies of the Franco regime by merging the Third Information Section of the High Chief Staff (AEM) with the Central Documentation Service (SECED) under the Presidency of the Government. That combination resulted in particular sections as follows:

> - Section of internal affairs, for the administration of the Service and the protection of classified materials.
>
> - Studies and reports section, for the acquisition, study, and use of any documentation of interest to the Presidency of the Government.
>
> - Coordination section, for permanent communication with regional delegations. Liaison officials worked in several ministerial departments, disseminating, and coordinating information (Almenara, 2012, p. 156).

Despite the institutional transformation, the CESID failed to prevent a military "coup d'état" in February 1982 by hardline security members (such as Antonio Tejero, lieutenant of the Civilian Guard, and San Martín, the former leader of the OCN information service). The coup d'état against the new democracy by the radical military was a desperate attempt to save "democracy itself", as well as to preserve "the monarchy and freedom in the country" against the corrosion of authority and the establishment of "chaos and disorder" (Palacios, 2001, p. 346). Rebels such as the high-ranked official José Cortina Prieto, who maintained contacts with the American CIA and the Vatican, tried to conspire openly against Adolfo Suarez. In this kind of conspiracy, the uprising can be interpreted in a gray zone, between the attempt to save the country from even more extremist groups from the military, and the attempt to redirect what Prieto and other rebels believed to be the wrong path in the transition process.

After the uprising against the new political order, the CESID fell into discredit and many directors took control of the Center. Yet, under the rule of Emilio Alonso Manglano (1981-1995) the information center experienced a period of long stability, which in terms of organizational procedures, consisted in a cycle of centralization, followed by a delegation process that concluded with a period of "coordination dilemmas within the information/intelligence community" two decades later (Díaz-Fernández, 2006, p. 29).

To collect personal and private information, the CESID deployed a network of officials across different Ministers or Executive Offices. For instance, since the OCN times, a direct communication channel was established between the "General Office of Security" (*Dirección General de Seguridad*) and the "General Office of Homeland Affairs" (*Dirección General de Política Interior*), as the latter offered hundreds of individual profiles and records collected by police agents across the country. It is worthy to mention that each of the Sections of the General Defense High Staff (*Secciones del Estado Mayor*) and the "General Police Department" (*Comisaría General de la Polícia*) also counted with agencies to collect sensitive information but their structures were "smaller" when compared to the SECED and the CESID ones (Peñaranda, 2005, p. 100).

During the transition, the Spaniards voted a Political Reform in 1977 that included a New Constitution and the first direct elections to the Parliament since the Civil War. Despite those structural political changes, the information community continued to reproduce old methods and practices. As a symbol of the legacy constraints that marked the information services, we can mention that surveillance practices promoted by the OCN were barely renovated during the SECED and CESID years. From 1974 to 1975, for example, the Information Bulletins that the SECED disseminated to the leaders of the Government, including the King, continued to report information about the political situation at schools and universities. For example, these documents reported teachers' and professors' activities for better contracts, as well as the strikes to maintain the status of autonomy at universities (Linz, 1981). Some of those strikes were not necessarily political complaints against the regime or acts of political dissidence. Yet, the reports prove that this field was under direct surveillance to the eyes of the information service as they continued to deploy vigilantes and infiltrate agents as in the times of the Franco era.

The information center also was concerned when the Spanish Communist Party (PCE) was legalized in 1977. Also, the SECED leaders wanted to contain social movements. For example, in their reports, they asked, "where is the most important place to restrain the "problem" [of subversion at the universities]? […] Where are the most conflictive university districts?" (Villar Cirujano, 2015, p. 113), among other issues. Yet, the information center also criticized other Ministries, as in the case of the delay to build a university hospital in Seville and condemned the

police brutality to neutralize the protests of students at the Faculty of Medicine in 1975 (Villar Cirujano, 2015). Many of those reports contained details and deep diagnoses of the political life in the country; a proof that surveillance was extensively used by the services. [20] However, they prove that surveillance alone was not enough to transform policies and practices of the government. The intrusive surveillance over target groups was used to support other security forces and the police, providing essential information for repression and the use of disproportional violence.[21] However, documents attest that surveillance had a little effect to contain the full extent of the social upheaval, such as the educational and labor protests in those years. Surveillance was not the mighty monster as in totalitarian states. Yet, it was fundamental to monitor the opposition and dictate, to a certain extent, the rhythm of the transition.

To redefine the rhythm and path of the transition, some authors emphasize the role of the information center to contain destabilization attacks, especially from terrorist groups during the late 1970s. For example,

> In the analysis of the phenomena that could endanger the regime, the SECED continued to extend its activity over trade unions, religious and intellectual groups. Activities designed to know the nature of the incipient Basque phenomenon and inherited from the OCN were added to those areas. The so-called Udaberri Plan, for example, sought to detect, delimit and understand the different elements and actors that created the Basque nationalism, an idea that still was not clear to the security services. In addition to the information actions, the SECED members conducted important operations against ETA, such as the Operation Lobo that in 1975 captured the leaders of the terrorist group, arresting 25% of the members. The SECED structure as well as the

[20] In terms of the information community during the Franco era, Law of March 15, 1940 (BOE No. 77) in its fifth Article reorganizes to the Civil Guard, among other tasks, "the surveillance and guard of the camps, towns, factories, industrial and mining centers, coasts and borders, the pursuit of contraband and fraud, and the foresight and repression of any subversive movement, and, at all times and in all places, the persecution of criminals". Meanwhile, "the Second Section of the High Chief Staff was the body responsible for the coordination of the Information Services of other organizations at the national level. The tasks that should be established in a regular base were: High Staff, regarding clandestine actions, information analysis from abroad, relations and staff with the American bases, espionage, sabotage, social conflicts, etc. The Second Section Bis of the Central High Chief Staff, focused on external military information, activities of personnel belonging to the Army, and information related to the Units of the Army. The Second Section Bis of the Air, in relation to suspect flights, air accidents, information related to the Air Bases and activities of Aviation personnel, etc. The Second Section of the Navy, regarding the information related to the Naval Bases, personnel of the Navy and movements of ships, boats dedicated to contraband, incidents in the ports, behavior of crew members, etc." (Peñaranda, 2005, p. 97).

[21] The SECED has been linked to far-right groups such as the Basque-Spanish Batallón or the guerrillas of Cristo Rey, and by extension, with the execution of violent actions. As indicated, the activity of SECED was characterized by focusing on gathering information and developing psychological operations rather than intervening directly in groups of interest. But although the SECED did not participate in this type of actions, it really provided this information in an ongoing base to groups such as those of Blas Piñar, who carried out violent actions, from beatings to murder (Díaz-Fernández, 2005, p. 211).

> personnel who worked against ETA were assimilated by the CESID two years later (Díaz-Fernández, 2005, p. 208).

As the attacks from groups like ETA hit several members of the Armed Forces, senior officials protested in their inner circles against the “lack of authority" in the new "democracy" to combat terrorism (Zaverucha, 1994, p. 51). Indeed, the Spanish transition entered a zone of tension, which was configured by the conspiracy of certain groups within the Armed Forces and the violent actions from ETA. The internal impasse between radical right groups and loyalist groups was only reduced after the failed Coup in 1982 and the electoral victory of the Socialist Party this year. In that sense, if there was no more reasons to fear the Jews and the Communists, as Franco supporters believed, the information services continued to monitor the political evolution from different groups in order to guarantee some stability to the transition (Palacios, 2001).

In that effort, another example of the SECED surveillance was a file system called “Janus”. This system stored hundreds of records about people who played a prominent role in the democratic transition -in favor of or against it. By including their two “faces”, the public and the private, the system enabled the “creation of complete profiles of politicians or suspects, including their properties and incomes” (Díaz-Fernández, 2006b, p. 27) resembling the Greek myth of a double-faced figure. In addition, the system relied on two major divisions that continued for decades: the Information and Operations divisions that, as mentioned above, were mainly deployed over labor, religion, and education. The divisions were also instructed by the Psychological Actions Office, the Department of Special Affairs, and by the General Secretariat; all of them provided valuable information including from open sources” (Zorzo Ferrer, 2005, p. 90).

Alongside the “Janus” System, the SECED used to collect information by other mechanisms. For example, as it depended on the Defense Office, the “Center” was supported in tasks such as "cryptanalysis and decryption by manual procedures and electronic means" (Ruiz Miguel, 2005, p. 138). To conduct those activities, surveillance organizations like the SECED obtained special funds of the national budget via the “General State Budget Law”. Whereas this rule established a percentage of resources to each national agency, complementary resources came from the “Reserved Funds”, a sort of monetary fund to cover Defense and National Security tasks. Compared to other national expenditures, the Reserved Funds were classified as official secrets regarding details and goals. Even nowadays, “Any information related to appropriation or the usage of the Funds is covered by secret classification" (Law 11/1995) and can only be declassified by the Council of Ministers or by petition of the Parliament.

Since 1981, under the supervision of director Emilio Alonso Manglano, those secret funds supported the expansion of the CESID. Years later, the Center

deployed information networks in broader points of the administration, covering these organizations:

> The Ministry of the Interior, the Ministry of Information and Tourism, Ministry of Education and Science, Trade Union Organization, Ministry of Labour, General Secretariat, the National Youth Delegation and the National Delegation of Women's Section. The exception was the Ministry of Foreign Affairs, presumably because information coming from abroad belonged to the High Command Staff of the Military (Peñaranda, 2005, p. 100).

The information network was a key element in the Spanish transition and there is no doubt that the biggest organization that gathered personal information was the CESID. After 1977, it monitored political radicalizations against the "top-down"' arranged transition. Later on, the CESID was a tool for monitoring the subsequent terrorist attacks from groups like the Basque ETA – especially during the "dirty war" in the 80s. As the democratization process was being consolidated, it was necessary to restrain previous practices that targeted politicians and citizens. In formal terms, it was essential to build more controls to tackle surveillance practices. In that sense, a phrase suggested by a former leader of the service, Gutierrez Mellado, summarizes that context: "the CESID simply could not wish to bring up the militaries towards a democratic culture. However, it was easier and convenient for them to obey the orders coming from the new political government" (Díaz-Fernández, 2006b, p. 213).

In 1976, in the context of the renovation of the information services, the journalist Eduardo Álvarez Puga wrote that parallel military forces were financed by Basque businessmen to combat ETA as they believed that this organization received funds from the Soviet Union (Encarnación, 2007). The paramilitary forces were in fact undercover operations between security forces and the extreme right that took place without any kind of government control –although it consented by indirect means. The parallel use of the police, the Civil Guard, and the information services to counteract adversaries are difficult to be detailed in terms of authors, facts, and objectives. Yet, some authors point out to connections between international groups, such as Italian neo-fascist squads who trained the Spanish information services, and the creation of anti-terrorist death-squads that tortured and killed rivals with impunity (Almenara, 2012). One of those death-squads was creatively named as the "Antiterrorism Liberation Group" (GAL). The GAL kidnapped and murdered 27 people in covered operations of the police in the Basque Country and in southern France from 1983 to 1987. The actions of this group were known by the information service as attested by the leaks that journalists released during the *CESID Papers* scandal in the 1990s (Encarnación, 2007). It can be said that the GAL was a sub-product or indirect ramification of SECED and CESID as the Spanish information service knew but ignored the GAL operations. Hence, disgusting and abject activities were promoted by omission

whereas the service tried to renovate its internal agents and doctrines during the so-called 'dirty war' of the 80s.

In 1985, the Spanish press denounced that the CESID intercepted communications from the president of the Cortes (Spanish Parliament), Gregorio Peces Barba, as well as from high government officials and parties such as the PA (Andulucian Party) and PCE (Spanish Comunist Party). The reports indicated cases of homosexuality, conjugal infidelity, pedophilia, marijuana dependence, as well as the construction of chalets and the purchase of tickets to travel abroad and to watch football matches at the expense of the public treasury (Almenara, 2012). Those reports aimed to monitor the political life of key leaders with no clear purposes. Yet, they show that, even in the renovation, old elements and doctrines would have persisted in the information service.

When the service tried do adapt itself to the new democratic regime, it was because Spain aimed to transform the internal political regime in a broader sense. In 1982, during the internationalization process that transformed Spain as a Western ally during the Cold War, Alonso Manglano developed the acknowledged Fénix Plan. This plan aimed to modernize and adapt both the structures and the objectives of the CESID to the internal and external needs of Spain in terms of intelligence (Díaz-Fernández, 2005). The Plan aimed to mitigate the involutions that could have stopped the transition, reinforcing counterintelligence, the technological capabilities, and the external intelligence cooperation. Due to the international pressure to assume a role in the North Atlantic Treaty Organization (NATO) and as part of the integration in the European Union, the new political scenario was very different from the Franco era (Aba-Catoira, 2002).

However, renovation of information services has always been, and not only in Spain, a battlefield with many fronts and situations. For example, in the 1980s, Díaz-Fernández (2005) affirms that CESID collided with other agencies to control the flows and outputs of information/intelligence. That is, CESID had conflicts against the Ministry of the Interior, Ministry of Defense, the Ministry of Foreign Affairs, and even against the Presidency. Those clashes shaped the CESID functions and actions to control the field of intelligence in Spain.

> Within the Ministry of the Interior, the police and the Civil Guard continued with their respective processes of modernization and democratization, while their information services faced important disputes with critical moments between the years 1988-1989. The disputes between both bodies were intense. The accusations included espionage between the ministries, the existence of infiltrated agents in the Ministry of Foreign Affairs, the sale of secrets by CESID officials, the spying of the police to politicians, including the president of Congress. There were also complaints about the failures in foreign cryptography, and police accusations to the government of being afraid if it took away

> any information competence from the military. Regardless of the assessment and even the veracity of this news, the hostility and confrontation between these services were evident as they sought to discredit their competitors in the struggle to get a piece in the field of strategic information (Díaz-Fernández, 2005, p. 261).

When the Cold War ended in 1989, the CESID scope and objectives expanded both quantitatively and qualitatively. Previous objectives such as antiterrorism and the security of the state added new tasks related to the complexification of threats, the technological changes, and the increasing international interdependence in matters from economics to environment. During the 1990s, however, two episodes marked the Center in a way that compromised its expansion and credibility. The first episode, the *SECED Papers*, relates to a series of documents leaked by "El Mundo" newspaper that compromised the operations and exposed the actions of the dirty war against terrorist groups (ETA and GRAPO) in the previous decade. The Center tried to achieve more reforms but it was affected by the leaks. The CESID suffered a paralysis of decision making as a consequence of the constant replacement of directors, and the changes in the political spectrum as the Socialist Party transferred the power to the right wing Popular Party in 1995.

It was during these years when parliamentary groups discussed stronger measures of accountability and control of intelligence (see next sections). In 1998, however, the center was hit by a second crisis because of the illegal eavesdropping on a Basque political party (EH Bildu) in the city of Vitoria Gasteiz. This event demonstrated the need to improve the legal controls of intelligence activity. As a result, in 2002, the CESID was transformed into the "National Intelligence Center" (*Centro Nacional de Inteligencia* – CNI). In this reform, the institution received a Cabinet Office, and the rank Director of the Center was updated to the rank of State Secretary. In addition, Legislative and Judicial controls were developed to check operations that interfere with the fundamental rights of citizens. We will address these accountability mechanisms in the next sections.

In November of 2003, during the movement of CNI agents between the Iraqi cities of Baghdad and Diwaniya, two vehicles were targeted by armed rebels that killed seven people. The massacre revealed the tactical errors and failures in the mission of the Spanish intelligence in Iraq and compromised the deployment of agents in the Middle East. One year later, on March 11, 2004, artifacts exploded in the Atocha train station in Madrid. This was considered the first and the most lethal terrorist attack in Spain after the so-called international War on Terror after 9/11. The critical hours that followed this event revealed the lack of coordination and even contradictory discourses between the Ministry of Interior and the CNI regarding the authors of the attacks. It was believed that ETA provoked the bombings, but police investigations and CNI agents attested that Spain was facing a

new threat. Nowadays, according to the official website of the CNI, terrorism, and, particularly, international terrorism is the biggest threat to intelligence services. This is a credible fact, especially if we consider that ETA declared a truce in 2006 and a definitive dissolution in 2017.

3.3.b. The Brazilian path: SNI, SAE, ABIN-SISBIN

After World War II, the military overthrew the dictator Getulio Vargas and started to be a veto player that intervened in political clashes During the New Republic (1945-1964). In the context of the political turmoil during this era, the military were invoked as guardians of stability and integrity. During the 50s, in a speech by one of the most popular politicians, Otávio Mangabeira, he stated: "The Nation is exhausted from so much humiliation and suffering. Only the Armed Forces can save the country. We the people are united as one man. We trust them and obey their command, as if we were at war" (Delgado & Ferreira, 2003, p. 308).

In that logic, the military interventions were considered as legitimate actions, especially when the political elites altered, to the eyes of the Armed Forces, the limits of legality and the public order. In that context, civilian sectors and the military created the Superior School of War (ESG) in 1949. In this institution, they formulated the "National Security Doctrine" as the ideology that served to promote the Coup D'état in 1964. According to the Doctrine, the political clashes of the Second Republic were something to be avoided "because they were a factor of internal division that broke the hierarchical structure of society, contaminating the military institutions with social conflicts" (Dreifuss & Dulci, 1983, p. 92). The Doctrine formulated the providential mission of saving the homeland and intervening in contexts of instability. In the ESG, the Armed Forces received a political rather than a military formation, fostering the emergence of the mentioned veto power role. In that sense, the military tried to convince the rest of the society about the key ideas of the doctrine: order, unity, nationalism, morality, and progress. Therefore, social antagonisms and ideologies that explain society by the perspective of class struggle and revolution were harmful to the interests of the nation. The expansion of the Doctrine caused the end of political pluralism during the dictatorship as explained in the previous section.

In institutional terms, the General Secretariat of the National Security Council of those times was not prepared for the new dynamics of the Cold War. That is, it was necessary to create an organization with the function of collecting and analyzing critical information to the country's defense. Decree 9775 of 1946 stated the President of the Republic as responsible for laying the foundations of war action plans. As part of these actions, through Decree 9775, the General Secretariat was divided into three Sections. The Second Section started to coordinate the

information between the Ministries and the first Brazilian information service: the "Federal Information and Counter Information Service" (SFICI).

During the 1960s, due to the escalation of the Cold War conflict the need for coordinating more information across the country increased. Antunes (2002) states that the SFICI strived to institutionalize its functions, such as monitoring communists and radical anarchists. At those times, the National Security Doctrine penetrated the information service. Parallel to the SFICI activities, the Armed Forced also created information services in the late 1960s to combat subversion in their three branches: the Navy Information Center (CENIMAR), the Army Information Center (CIE) and the Aviation Information and Security Center (CISA). This reforms institutionalized the National Security Doctrine in order to stop the subversion.

After the military coup d'état in 1964, General Collbery de Couto e Silva asked President Castello Branco to present a project for the creation of a new information service. Couto e Silva expressed that a solid information system was one of the key actions to consolidate the new regime (Antunes, 2002). The National Information Service (SNI), enacted by Law of June 13, 1964, was created under the Presidency of the Republic to operate on behalf of the President and the National Security Council. According to the Law, the purpose of the center was:

> […] To assist the President of the Republic, guiding and coordinating information and counter-information activities, […] establishing and ensuring the necessary understandings and liaison with state governments, private entities, and municipal administrations; […] To coordinate information to the decisions of the President of the Republic and the National Security Council (CSN), and to promote the adequate dissemination of information. (Law of June 13, 1964)

The SNI was essential to the decision-making and the survival of the regime. According to the law, the SNI chief obtained ministerial prerogatives and was appointed with the consent of the Federal Senate. According to internal regulations (Decree 55.194, 1964), delegations in the states of the Federation were created to support the information analysis executed in the headquarters of Rio de Janeiro, the former capital of Brazil. Those rules allowed the SNI to implement and expand its sub-units across the country.

In terms of internal organization, different sections comprised the SNI, such as:

> The strategic information section, which was created to conduct data research following the instructions of the Chief or Head of the Service. Meanwhile, the Internal Security Section was created to identify and evaluate the current or potential antagonisms that could affect national security (Antunes, 2002, p. 56).

By 1967, the SNI structure expanded again. The former National Security Sections were transformed into "Security and Information Divisions" (ISDs). The link with other Ministries, as well as with the information services of the Armed Forces, resulted in a vertiginous expansion of the Service. The SNI became a powerful organization, the main node of the great network of information services during the military regime, receiving greater resources and operative capacities each year.

During the Medici administration, the Executive created the Information National Plans to optimize the collection and dissemination of information. The first plan was promoted by the SNI itself and enacted the National Information System, a network of channels to explore and regulate the flows of information. The Plan received objectives outlined by the President of the Republic and by the National Security Council. With the victory over the Araguaia guerrilla in 1974, the period of the armed conflict started in 1968 ended. This was a chance to review some of the assumptions related to the National Security Doctrine. However, during the administration of Joao Baptista Figueiredo, former Chief of the SNI from 1974 to 1978, the direct link between the information service and the government reached a new level (Antunes, 2002). The link allowed a new expansion of the service as General Octavio Medeiros and General Newton Cruz, Chiefs of the Service, received more human and financial resources from the Executive office. In those years, the SNI had reached extraordinary levels of reputation and was labeled as the fourth Armed Force (Soares, D'Araujo, & Castro, 1995).

Regarding surveillance practices that involved the SNI and other security agencies, the Brazilian Army structured operational divisions addressing internal monitoring in the country. Those divisions were called Centers of Operations and Internal Defense (CODIs) and Divisions of Internal Operations (DOIs). Both organizational divisions followed the guidelines for internal defense established by the National Security Doctrine. The DOI-CODI system did not work in a permanent base because the structure depended on informal contacts between the Armed Forces, the state governors, and police leaders (Rego, 1984). Yet, according to General Moraes Rego, DOIs were subordinated to CODIs and they served as tactical groups inspired by the Bandeirante Operation (OBAN)[22]; a series of actions carried out by the military police of Sao Paulo to hunt and exterminate political dissidents.

As in the case of the Spanish OCN, Gaspari (2014) affirms that, since 1964, police institutions - civilian and military - had no conditions to control the "Marxist penetration within the organs and communication of the public administration". Thus, according to him, the military has been forced to fight subversion by

[22] OBAN emulated the ancient Paulist "destiny" policy of expanding the territory and seek for fortunes at the expanse of indigenous massacres during the colonial period (Joffily, No centro da engrenagem. Os interrogatórios na Operação Bandeirante e no DOI de São Paulo (1969-1975), 2013).

exceptional means. In that sense, and to accomplish their missions, DOIs received support from various sectors: the military police, the federal police, as well as members from the Armed Forces (army, navy, and aeronautics). Yet, CODI-DOIs maintained a high degree of autonomy, conducting undercover operations, and infiltration tactics (Fico, 2001). For example, CODI-DOIs officials wore plain clothes and infiltrated agents to undermine target groups. The Divisions owned places to arrest people and prosecute individuals with total discretion. For those practices, civilians nowadays associate CODI-DOIs with places of repression and torture during the regime. In that sense, the work conducted by the police overlapped the one conducted by CODI-DOI agents, especially because there was a total convergence between policing the public order and preserving national security (Fico, 2001).

General Fiuza described the operations conducted by the DOIs as follows:

> The DOI picks up, holds, and interrogates... For capturing and individual, the Divisions deploy lieutenants, captains, but the main group is formed by sergeants. After arresting someone, information about the target is passed to the Second Section of the Army, which has about 10-15 specialized officials working all the time... In the interrogation process, the questions need to be conducted by a calmed, intelligent, and firm agent while a superior oversees the whole situation... Those who are suspicious or need "to be treated" go to the spreadsheet ... People are arrested for 30 days, being 10 days with no external communication (D'Araújo, Soares, & Castro, 1994, p. 61).

Antunes (2002) also affirms that the CODI-DOIs became the main network for clandestine operations, repression, and torture. This is even clearer as recent documents (released by the State Office of the United States of America) attest that the upper ranks of the Armed Forces, despite denying the use of torture, already knew the existence of CODI-DOIs operations (US State Office, in Joffily, 2019). However, we must be careful to assert that any action of torture or repression was directly associated with the SNI and strategic information services. Some cases of torture were probably conducted informally, with no direct implication of SNI information structures. Yet, this does not excuse that the Service exercised a key role in the use and sharing of information with DOI-CODIS. For example, in 1971, during the Mesopotamia Operation conducted in the northern Maranhao state, reports described individuals who should be arrested even before the start of the operation (Mechi, 2015). These reports also established *a priori* forms of accusation, prosecution, and techniques to suppress the subversion. For example, interrogators already expected certain kinds of information during the process of torture according to questionnaires formulated by the CIE, one of the branches of the SNI. This trend exemplifies the inquisitional characteristics adopted to prosecute "suspects"- They also represent a legacy constrain or institutional path

that left a remarkable heritage to police operations even nowadays (Yauri-Miranda, 2019).

However, as in the Spanish case, the activities of the information community must not be taken as a totalitarian rationalized network for oppression and systematic abuse. The abuses existed but the coordination of the system was also informal and depended on many factors. For example, there were many parallel hierarchical ranks within the system, as well as duplicity of functions on a large scale. CODI-DOIs network also depended on personal contacts to gather and disseminate information to the information services of the Armed Forces and to the SNI (Antunes, 2002). In fact, this loose and informal network turned difficult to establish an efficient and internal control of the organizational structure by the military. That explains, in part, why the information community acted with impunity especially during the darker years of the regime, extrapolating the functions of an information service and developing a large police/operational sector that resembles international cases, such as the postwar Polish Ministry of Public Security (MBP) and the Soviet Committee for State Security (KGB).

Even if the violence of the regime is not attributed solely to the SNI, the service contributed the suppress citizens' rights and their autonomy. For example, the SNI intercepted mails, robbed documents, tapped telephone lines, and monitored thousands of people, especially political opponents, subversion suspects, and members of the regime bureaucratic apparatus. The SNI also infiltrated people in clandestine groups and legal organizations, such as the controlled opposition party MDB, trade unions, and student movements (Castro & D'Araujo, 2001). Even the Catholic Church became the focus of attention by the service after the AI-5. Bishops of the liberation theology, such as Helder Cámara and Pedal Casaldáliga, who supported land redistribution and human rights, also became targets of the SNI official gaze (Gomes, 2014).

In other words, the SNI organized, systematized, tracked, and investigated potential elements not only related to subversion. As the institution attempted to "defend" national interests in a context marked by the Cold War, it contributed to creating the stigma of the external and internal threat related to communism. That is, there was an overreaction to an ideology that was understood as the cause of an imminent total war in the conflict between the two Superpowers. It could be said that, according to this idea, several schools of command have been responsible for creating one mythology related to the Doctrine of National Security State: a permanent vigilant state to stop and eliminate internal "enemies". This kind of mythology or absolute position was promoted over other interests, including alternative political values, and over people that were not necessarily violent and dangerous.

As the “slow, gradual and secure” process of distention was announced by the military, the political transition opened internal “cleavages” within the regime –i.e. officials intending to remain in power from those who wanted to restore civilian rule and return to the barracks. When the military President Ernesto Geisel promoted the political “*abertura*” of the regime in 1974, this path was considered as a setback in the “revolution of 1964” by hardline militaries. For example, a critical situation occurred during the struggle for the succession of Geisel, who confronted the Chief of the SNI, General João Figueiredo, against the hardline Army Minister, General Sylvio Frota. The information services under the management of those generals -respectively the SNI and the CIE- were also involved in a dispute as they tried to increase their positions and resources at the expense of the opposing organization. Geisel sealed this dispute with the dismissal of Frota on October 12, 1977. After this event, the Army Minister considered that the distension process was a betrayal and a left-turn in the history of the country. This internal division is supported by researchers such as De Oliveira (1987), who believes that if democratic aspects did not reach the whole military apparatus, neither was the case of authoritarian aspects. That is, there was not a totalizing ideology or doctrine within the military despite their authoritarian convergence.

When João Figueiredo received the Presidency in March 1979, the most repressive legislation, the AI-5, was already abolished in December 1978 as the outbreak of student and worker strikes accelerated the democratization transition. Nevertheless, during the 80s, hardliners planned attacks to destabilize the political transition and created ways to take control (again) of the country. For example, bombing attacks in Sao Paulo were attributed to General Milton Tavares as an attempt to blame leftist groups and invoke the old National Security Doctrine. In Rio de Janeiro, bombs exploded on newsstands, in the Brazilian Press Association (ABI), in the Brazilian Lawyers Association (OAB) and Riocentro. According to General Zenildo Lucena, these attacks were the responsibility of General Newton Cruz, head of SNI Central Agency (Castro & D'Araujo, 2001).

When General Joao Figueiredo's administration ended in 1985, the new period of democratization demanded the redefinition of surveillance activities for the sake of the new republic. During the civilian government of José Sarney, the internal National Security Doctrine and the fight against international communism were in decline so as the very antagonisms of the Cold War. Therefore, the SNI Chief, general Ivan de Souza Mendes, was forced to review the information methods. According to him, the Service started to focus on new and external problems, such as international and economic espionage, and territorial and border problems (Antunes, 2002). However, in 1987, according to General Carlos Tinoco, the SNI was still preparing briefs that summarized the situation of subversion in Brazil (Castro & D'Araujo, 2001). In addition, during the 1989 presidential election, the service infiltrated agents at the Sixth National Meeting of the Workers Party (Partido dos Trabalhadores - PT) (Sarkis & Novais, 1994).

The SNI was not altered during the 1988 constitutional reform, in which the main political concern of legislators was to balance the civilian-military relations and to restore social rights that were abolished in the Constitution of 1967. However, when Fernando Collor de Mello defeated the Workers Party (PT) and obtained the Presidency (1990-1992), he enacted an Executive Decree that abolished the SNI in 1990. This action was understood as personal revenge against the work of the information service as it aimed to undermine Collor's reputation during his running campaign to the Presidency. To replace the SNI, Collor created the "Strategic Affairs Secretariat" (SAE) despite the resistance and pressure of the military and public officials. According to Flores (Flores, 1992), one of the leaders of the Secretariat, the new organization downsized its staff and emphasized foreign intelligence, making analyzes of open sources and obtaining information from similar foreign organizations. Flores also affirmed that the SAE started to monitor transnational crimes, new forms of terrorism, and drug trafficking. Regarding internal surveillance, the Admiral mentioned that the Secretariat was an "apolitical public service" (Antunes, 2002, p. 108). However, the press of that time contradicts his statement. In 1994, when the newspaper "Gazeta Mercantil" uncovered the vigilance exercised over political parties, Admiral Flores tried to justify the monitoring of PT and PSDB, as well as the monitoring of favelas and land invasions in the North of the country, deeming those issues as "very important to the country's security" (Antunes, 2002, p. 110).

The repetition of "old doctrines" in the new Secretariat can be understood as an indicator of legacy constraints or past legacies that the SNI inherited to the new organization. The legacy is also explained by the lack of regulation to edit the intelligence activity during the 1990s. The lack of administrative and legislative measures to regulate intelligence did not mean total silence by politicians and society. Several legislators proposed projects in that decade, a trend that we will address in the next section on legislative control of intelligence.

On December 7, 1999, President Fernando Henrique Cardoso sanctioned Law 9.883, which established the Brazilian Intelligence System (SISBIN) and regulated the creation of the Brazilian Intelligence Agency (ABIN). Officially, it was the first time that the word "intelligence" appeared in the nomenclature of this activity. The SISBIN was created to integrate the planning and execution of intelligence activities at the federal level, establishing the idea of a network or official intelligence community. In the meantime, the ABIN would become the "brain" of this network, the main collecting node, and the chief organization of the SISBIN. When Congress passed this, criticism remained as the legislation did not regulate the ABIN role within the system. For example, there was not a word mentioning the integration of policing intelligence, especially if we consider that public safety and organized crime became new priorities of the intelligence community after the Cold War. All the same, the regulation introduced a necessary milestone to synchronize the area of intelligence with the new constitutional

regime, for example, by demanding for the first time a legislative commission to oversee the ABIN. The new agency aimed to wash away the SNI reputation of abuses and deviation of power by emphasizing that intelligence "is to be developed […] with the unrestricted observance of individual rights and guarantees, fidelity to the institutions and ethical principles that govern the interests and security of the State" (Law 9.883, articles 3-5).

The attempt to democratize and put the SNI legacy in the past was also a response to a series of incidents that hampered the intelligence as a key process for policymakers. In 2008, the Brazilian Intelligence Agency (ABIN) was involved in a series of political espionage and illegal collusion with the Federal Police to prosecute financial crimes, such as in the *Operation Chacal* and *Operation Satiagraha*. A group of ABIN agents and staff from a telecommunication company in Rio de Janeiro (TELERJ) were held responsible for the so-called "Cayman Dossier", a set of false documents created to prove illegal accounts from politicians linked to the Social Democracy Brazilian Party (PSDB) (Zaverucha, 2008). Moreover, during the last years, the Edward Snowden revelations have shown the monitoring capacities by the US National Security Agency (NSA) and the ABIN inability to deploy counter-intelligence measures to guarantee the security of communications of key leaders and politicians (Carpentieri, 2016). This deficit probably explains the removal of foreign intelligence and technology sections from the ABIN to the military intelligence, and the functional submission to the Institutional Security Cabinet (GSI), a military house linked directly to the President that oversees ABIN activities. Finally, the "Intelligence Policy" and the "National Intelligence Plan" from 2012 and 2015 increased the autonomy and scope of intelligence agencies, including the ABIN. Those years seen a controversial autonomy that intelligence agencies used in the past, in which they often acted without the supervision of the Executive itself. Besides, "The National Intelligence Plan" was formulated to preserve the interest of the nation even if those interests are vaguely formulated and defended especially by the military. In that sense, it is difficult to synchronize the intelligence activities between the Constitutional Order, in the sense of state, with contingent measures established by each President. Since 2017, the last presidential term has seen the reinforcement of the military scope over the ABIN mandates, reminding a combination of ingredients that was used during the SNI years. This is the case, for example, of the direct use of agents to monitor environmental pressure groups and Brazilian diplomats in international forums in recent years[23], and the alleged use of a structure from the ABIN to defend the Bolsonaro clan in corruption investigations[24]. Considering this

[23] Lo, J. 2020, October 14, 'Brazilian spies intimidated government's own delegates at climate talks', Climate Home News. Retrieved from https://www.hispantv.com/noticias/brasil/479155/bolsonaro-agentes-secretos-espionaje-cop25 in 11/13/2020.

[24] Últimas Noticias, 2020 December 11. 'They ask to investigate if Brazilian intelligence helped Bolsonaro's son', retrieved from https://en.ultimasnoticias.com.ve/news/general/They-ask-to-investigate-if-Brazilian-intelligence-helped-Bolsonaro%27s-son/ in 12/14/2020

continuous dispute of forces, it is necessary to scrutinize the accountability mechanisms deployed upon the intelligence activity in the next sections.

Epilogue

So far, we have depicted the institutional paths and evolution of the Spanish and Brazilian information/intelligence communities. In both countries, the military elites wanted to exercise their hegemony over this strategic activity during the end of the military regimes and during the transition process.

In the first case, the Spanish military aimed to maintain intelligence under their control to guide the democratization path or at least to preserve this arena as their "natural" domain. As Numeriano (2007) affirms, the military were oriented by two principles: a) they considered the information service as an institution of "their" scope, a domain that should be organically and operationally subordinated to the Armed Forces; and, b) the area of information/intelligence was a strategic source to obtain relevance or political power during the transition.

In the Spanish transition, the SECED and the CESID were recipients of the Francoist regime ideology, but, at the same time, they were influential actors in the reform of the regime. The CESID did not emanate, like the Brazilian SNI, a Doctrine of National Security to orient practices and methods. Yet, the CESID was progressively embodying a dualistic political-ideological position. The service served as a front to support the transition against the military and civilian elites that were refractory to democratization. At the same time, the CESID was a zone of entrenchment of the military that implemented the motto "change to preserve". Probably, this is a typical pattern of institutional actors in the internal transition of information services. The legacies of the previous order resisted and influenced the design of new institutional changes. For example, even when CESID was transformed into the CNI in 2002, the military strived to maintain the organic dependence of the Center to the Ministry of Defense. In each reform, the clash of factions and the internal cleavages were inserted in a top-down policy process. In that sense, each new redefinition in this arena did not affect automatically the characteristics attached to intelligence (either as a procedure or as an organizational sector). In each change, the power of the main information/intelligence agency was bargained against other security and strategic apparatus within the state –such as Interior, Foreign Relations, and Defense. As a result, the national intelligence agency prevailed as a key component for the reconfiguration of the state itself. Yet, as we will see, it is still necessary to assess if those changes were complemented with a deeper control and oversight of intelligence.

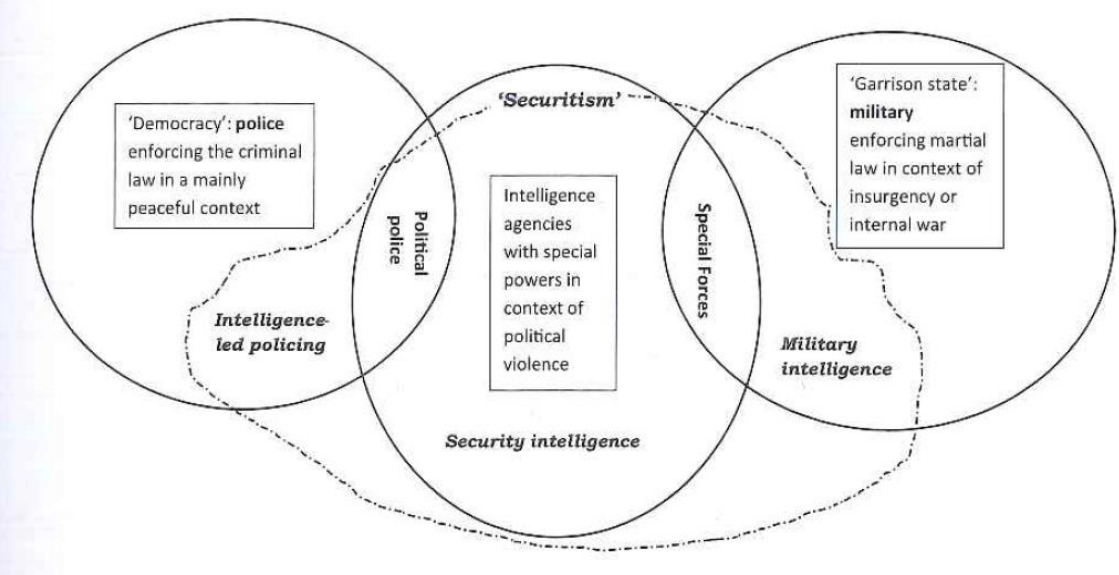
In the case of Brazil, when the transition started, the military had already a prominent role in the information community as well as in the political path of the country. The military took control of the political life and submitted it to the National Security Doctrine. As a result, the Brazilian military had their role as masters of the information services unquestioned. Due to their prominence in this realm, the most significant challenge consisted of restraining the military to allow the gradual "*abertura*" process. As in the Spanish case, different factions emerged to regulate the rhythm of the transition, with some groups reacting negatively and committing attacks to create new menaces to justify the interventionist characteristic of the Armed Forces.

When the Spanish CESID expanded its range during the years of the Fénix Plan and obtained relevance to accelerate the integration of Spain into the NATO and the EU, the Brazilian SNI was already a mega-structure both in institutional and operative terms. The reputation as the Fourth Armed Force, and the fact that two of the Presidents of the Republic emerged from this organization, attested its capacity to gather and process information within the country. For this reason, even when the democratization process started and the civilian returned to command the country, the information service continued to practice old methods that resembled the fight against the internal enemy. The official extinction of the service in 1990 and the creation of the ABIN in 1999 also suggest that the political vacuum and the stigma of this activity were difficult to be filled and managed during that decade. After the creation of the ABIN and the Brazilian Intelligence System (SISBIN), new challenges emerged in terms of cooperation, legal mandates, and external controls to oversee a realm that was not anymore a giant organization.

In both countries, the information/intelligence agencies have configured a trend called by some scholars as "security intelligence" (Hill, 2016). It means that those organizations acquired special powers in the context of political violence and extended their range of action to criminal prosecution and the defense of the country. The security intelligence agencies were a sort of "transmission belt" because they congregated and executed policies that blurred with the traditional roles from the police institutions and the Armed Forces. Intelligence, in that sense, performed tasks that usually were attributed to a political police and Special Forces. Proof of that link is the fact that both the OCN (predecessor of CESED) in Spain and the SNI in Brazil were created in a context where neither police nor the military was capable to manage the "problem of subversion" during the late 1960s. As a connector of methods and resources between police and soldiers, the information agencies collaborated or assisted in the soft and the hard suppression of dissidents and enemies of the state, as well as in the use of death squad and Special Forces to restrain the subversion. For those reasons, during the transition of the regimes, it was difficult to reestablish a peaceful scenario where the mandates of police institutions were supposed to be limited to the criminal law. At

the same time, until the 1990s, the countries promoted a sort of "garrison state" in which the military were supposed to enforce exceptional measures to counteract insurgency in an internal war (See Figure 7). Intelligence, centralized in the SECED/CESID in Spain, and in the SNI in Brazil, assumed key functions from the peripheral security institutions, expanding the "empire of intelligence" to other areas (as represented by the dotted area in the figure). This expansion turned difficult, if not impossible, to reduce the influence and the legacies of intelligence in the prospective life of security institutions in these countries. Once more, the constraint legacies explain, in part, that the forms to create institutions, the choices taken to configure their designs, as well as the praxis of the organizations, matter to understand why some vicious circles and deviations of power continued to be reproduced even in more democratic scenarios.

Figure 7: Intelligence expanding empire, or the intelligence amoeba, take one.



Source: (Gill, 2016, p. 61)

Furthermore, it is known that the merits of intelligence agencies are not commented and their failures are trumpeted. But an intelligence analyst and practitioner must deal with this characteristic in the reversal sense: the fact that mistakes are trumpeted indicates that new merits can be promoted especially after failures. As many public organizations, the merits are silent and related to the expected goals embedded in legal mandates and to the execution of decisions to solve social demands. In these circumstances, failures are expected to remain as abnormal or punctual events rather than continuous bases. Besides, an assumption that should be clear to intelligence practitioners is that they would not control every menace that emerges against the state and society. It is impossible to reduce all the variables and complexity of social reality to construct an intelligence product. In that sense, the merits are not only the merits of the organization. The security of the state depend also on contingent events and to a series of factors and

phenomena that scape from the best intelligence analysis. Thus, some failures are not necessarily mistakes of the agency and should be expected. Yet, even these unknown or unforeseen failures must be trumpeted because they bring the opportunity to redefine and readapt the intelligence institutional paths in order to leave legacies and constraints that affect the integrity of this activity. A failure is a painful yet privileged chance of reconstruction. And, to reconstruct these services, overreaction and deviation of power should be avoided because ultimately they would conduct to other failures that in turn would be trumpeted.

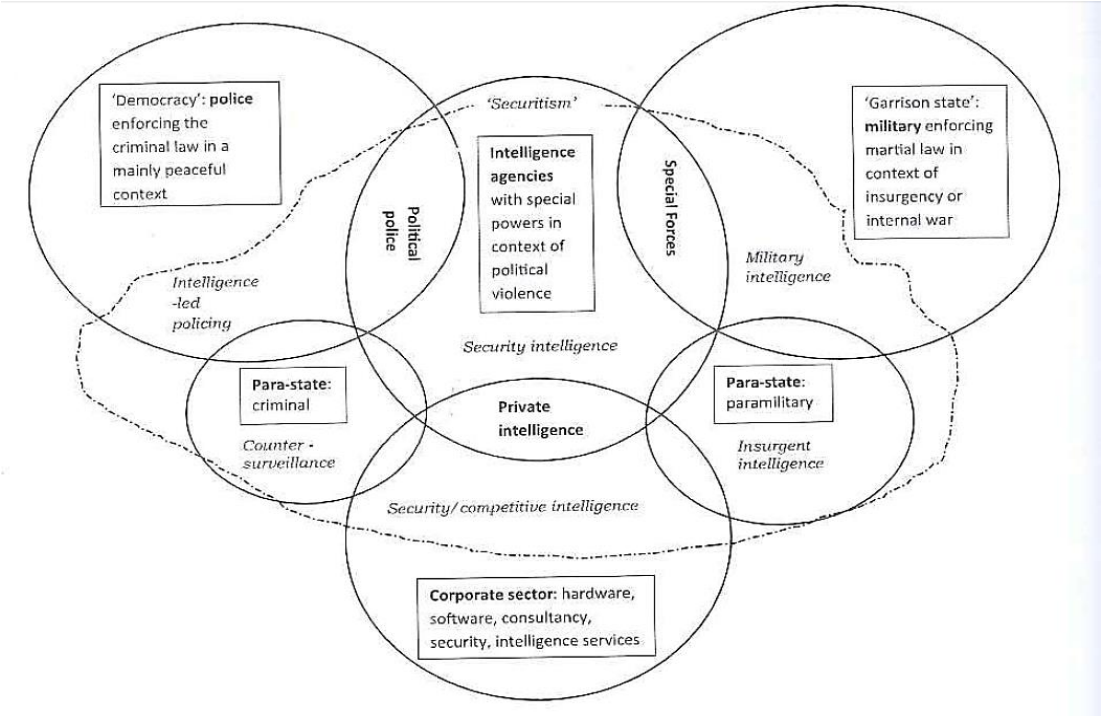
This section has shown that the information communities in both countries have similar dilemmas in terms of modernization and efficiency. We emphasized that both Spanish and Brazilian intelligence institutions were in a blurred line between active/passive players that helped in the surveillance of populations, shared information that included political monitoring, forced detentions, and sometimes tortures and executions. Historically speaking, those actions were mistakes that are to be trumpeted every day by practitioners and masters of this activity as examples to be avoided. For the non-practitioners, one must be cautious in associating every deviation of power and disgusting policy to these institutions. These institutions were not the rational machines of totalitarian states, nor were "improvised" and provisional solutions to the problem of subversion, political dissidence, or terrorism. The institutionalization of information/intelligence agencies represented the construction of coherent answers that states used to the deployment of "exceptional" measures. This discretional capability instrumentalized by contemporary bureaucracies can be understood as the epitome of sovereign power that demanded specific information for the integrity and continuity of the socio-political order. However, as we exposed, to preserve that order, intelligence tasks can sometimes contradict the very sociopolitical order, especially when the foundations of the order change –as in the case of political transitions- or when sovereignty collides disproportionally and unnecessarily against individuals within a territory.

Today, intelligence agencies must be calibrated through many mechanisms and dimensions. In that sense, scholars such as Eduardo Estevez divides intelligence into 1) intelligence to protect the constitutional order; 2) internal security intelligence and 3) police or criminal intelligence (Estévez, 2000). Intelligence for constitutional protection concerns the processing of information related, for example, to individuals and organizations that have among their objectives: to change or modify the constitutional order and the authorities designated by this order. In parallel, they "might" act against such authorities, to prevent the illegitimate exercise of those authorities if they carry out their duties through illegal and unconstitutional means. Internal Security Intelligence is linked with the processing of information related to individuals and organizations that pose a significant risk to the internal security of the country. This point should not be mistaken with unchecked and disproportional surveillance deployed upon

legitimate political activities, such as social protests, freedom of expression, political association, and so on. Internal intelligence does not necessarily means disgusting surveillance. Finally, police Intelligence, according to Estevez, is carried out to support the investigation of crimes and can be understood as a tool of daily use in the fight against minor and organized crime. There is no theoretical consensus as to what extent police intelligence differs from internal intelligence, especially when it comes to apply intelligence to crimes that are complex. Notwithstanding, in the above-mentioned definitions, the further we move away from the conceptual dimension and approach the practice, the more difficult it becomes to identify the boundaries between the several "intelligences". Yet, this highlights the importance of defining legal mandates among those subfields.

Considering the amoeba as an expansive metaphor made by an organism that extends its “arms” as in the previous figure, a new scenario has to be depicted in the last years (see Figure 8). Aside of the traditional connection and the expansion to police and military arenas, intelligence should lead with other areas such as criminal groups of large scale (counter-surveillance), para-state organizations that compete with the state (insurgent intelligence), and private organizations from different countries (competitive intelligence) that supply hardware, software and offer consultancy to state security intelligence agencies. This new scenario also blurs the traditional distinction between external and internal intelligence. In the external dimension, intelligence recognizes military aggression, espionage, territorial invasion, and economic subjugation as plausible threats. In the internal dimension, the threats represent the domestic support to the previous external threats plus the still problematic notion of “subversion”. As both the external and internal dimensions overlap, and new players emerge, intelligence must lead with uncertainty and new risks. Even when some threats are legitimate to be mitigated, such as organized crime and terrorism, those practices never emerge with clear lines or as pure ideal objects. For example, they could overlap with classical notions of political dissidence that seek for a dramatic change in the constitutional order. As constitutional orders are not eternal, and political changes are part of the historical contingency, the use of subfield divisions and legal notions matters but it should be constantly updated. Thus, the balance between ideal and practical lines, or the identification of discernible threats and the government answers based on intelligence, is still important but critical.

Figure 8: Intelligence expanding empire, or the intelligence amoeba, take two.



Source: (Gill, 2016, p. 74)

To accomplish their missions, both the Spanish and Brazilian information agencies were created in the 1960s by the messianic logic of saving the country against "internal enemies". Nowadays, what remains of that logic? As the notion of state security does not necessarily correspond with the notion of security of populations –because a state is not the mere sum of their habitants, nor people constitute automatically an state, and because the state might clash against their citizens beyond the obligations of public safety and criminal prosecution–; we also should calibrate the authority operated by intelligence institutions and the legitimacy granted to them by citizens in a broader sense. This balance can be done from permanents and strong legal mandates to unexpected and intermittent forms of citizens. To achieve this, the connection between authority and legitimacy, which is fundamental to an accountability action, needs to be explored and assessed from different perspectives. In light of that, the next sections deep into the institutional designs and functions of intelligence agencies in Spain and Brazil, showing the array of accountability mechanisms to tame these institutions: Internal control, legislative control, judicial control, the international level of intelligence cooperation, and the role of media and citizens.

3.4. Internal control

Internal control refers to the fact that the Executive power can demand accountability from its own services. In this section we trace the evolution, the current forms and the challenges to achieve this kind of control.

In Spain, on July 14, 1977, the CESID was created from the combination of the "Third Information Section of the High General Staff" and the "Central Documentation Service" (SECED), which was responsible for internal intelligence and anti-terrorism. However, there was not an internal regulation or a specific legal framework to control CESID activities.

Royal Decree 135 of 1985, enacted almost ten years later, was the first mechanism to regulate the Center. In those years, the functions of the CESID and other organizations -essentially military- were distributed and adjusted by their ministries. In the new democratic paradigm, it was evident that institutions such as information services needed their competences to be settled within the whole Administration. The lack of those mandates showed that "the Spanish intelligence service was created in 1977 without a real definition of functions and structure" (Díaz-Fernández, 2006b, p. 216).

The 1985 Decree restructured the Ministry of Defense, indicating the Higher Information Center of Defense as the body of the President of the Government responsible for managing defense policies and coordinating the protection of the state institutions. Article 2 to 7 expressed that The Higher Information Center of Defense had the generic mission of obtaining, evaluating, interpreting, and disseminating information in the areas of foreign intelligence, counterintelligence, internal intelligence, economy, and technology.[25]

At the same time, the CESID collaborated and coordinated, alongside the Ministry of the Interior, the defense of the constitutional order, and the domestic

[25] "Article 4: The foreign intelligence division responsibility is to obtain, evaluate and disseminate the information in order to prevent any danger, threat or external aggression against the independence or territorial integrity of Spain, assuring its national interests. Such information will cover the political, economic and military fields. Article 5: It is the responsibility of the counterintelligence division to oppose espionage and the activities of foreign intelligence services that attempt against national security or interests, through their prevention, detection, and neutralization inside and outside the national territory. Article 6: It is the responsibility of the internal intelligence division to obtain, evaluate and disseminate information related to internal processes that, through unconstitutional procedures, attempt against the unity of Spain and the stability of its institutions. Article 7: It is up to the economy and technology division to obtain, evaluate and disseminate the necessary information to prevent any danger, threat or external aggression against the Spanish industry and trade of armaments and war material and to ensure national interests in fields such as economy and technology that are relevant for defense, as well as ensuring the security of information, technology, procedures, objectives, and facilities for defense of Spain and allied countries" (Royal Decree 135 of 1985).

security (Art. 13). However, the coordination of those policies is a matter that has changed according to the circumstances and evolution of the Center.

According to Díaz-Fernández (2006), the CESID experienced five phases that correspond to the evolution of organizations according to Herbert Minztberg's theory. The phases relate to core values such as creativity, direction, delegation, coordination, and collaboration. After the CESID creation, monitoring the initial transition required a sense of improvisation in many tasks, as there was a lack of external regulation to coordinate the overall organization. In this phase, creativity was as important as trust and discipline within the information center. In a second moment, After Alonso Manglano took control of the Center in 1982, the direction phase served to strengthen the institution in the face of other organizations and the government. The aforementioned Decree of 1985 and the Fenix Plan of Manglano reflect this phase of rationalization of bureaucracy. In a third phase, during the 90s, the CESID reached a significant complexity, but during the exponential expansion of tasks and procedures, Director Manglano lost control over the "beast". In a fourth moment, after 1995, the specialization of CESID was replaced by a phase of coordination that put on the table dilemmas about its efficiency and political use. For example, the Center was used to conduct illegal wiretapping and surveillance of political parties.

> In May 1995, the press revealed that the Center had been conducting illegal interceptions. Thus, the credibility of the intelligence service collapsed to the eyes of media, political players, and economic groups. Weakened, the intelligence service was used to undermine President González position. The intense attacks led to the resignation of the Vice President of the Government, Narcís Serra, of the Minister of Defense, Julián García Vargas, and the dismissal of the director of the Center, Emilio Alonso Manglano (Díaz-Fernández, 2006, p. 30).

As attested by the quotation, the Center appeared in several scandals and cases of power abuse. The controversial collaboration with political repression in the past was replaced by the partisan use of the center to conduct illegal espionage against political figures. However, this also confirms that the Centre reached a level of importance in which the problems of the Center caused a turmoil in the political life of the country as a whole –which in turn caused the dismissal of key persons in the government, including the Director of the Center. We will return to the role of the media in section 3.8.

After the general elections in 1996, General Javier Calderón was appointed by the new government to reorganize the service. In this phase, the coordination between different divisions was not achieved since the creation of internal and external accountability controls was the priority of those years. However, before the CESID recovered its image from the eavesdropping scandal, in March 1998, the press revealed that the Center was also intercepting the communications of Herri

Batasuna, a Basque nationalist political party. The news released information from documents stolen by Colonel Perote, causing tremendous damage to the intelligence service. The Center did not know the extension of the leaks and canceled its operations and links with other services both inside and outside of the Basque Country. Moreover, foreign intelligence services expressed their deep concern about the CESID situation and restricted the flow of information to the Spanish intelligence service.

At the end of the 1990s, those events fostered proposals to reform and create a new intelligence center. However, the Center was refractory to lose its hegemonic place in the intelligence community. The Center's counter-reacted the reforming proposals based on technical arguments. For example, for the CESID, a reform to put the service under the direct dependency of the President would not be operational, since this would compromise the flow of information between intelligence and police institutions. At the same time, the CESID was looking for legal and judicial coverage to carry out operations, including those ones in foreign countries (Ruiz Miguel, 2005).

Resistance to reforms did not prevent, however, to keep the Center subordinated to the Ministry of Defense and to create an internal control under the rule of the first vice-president. This control aimed to establish civilian supervision over this strategic realm. Reform discussions continued throughout 1998 and 1999, focusing on processes and institutions to control the CESID activity. According to Díaz-Fernández (2005), two models were confronted. The presidential model, advocated by the vice-president Alvarez Cascos, proposed to split the CESID in different services, reducing its size and establishing Cascos as the coordinator of the new community of intelligence. The other model, defended by the Minister of Defense, Eduardo Serra, translated the CESID position to resists the reforms. Serra insisted that the CESID needed to preserve its position as the center of the intelligence system. He also argued that assigning services to the presidency of the government (direct subordination to the President of Government) would reduce the effectiveness of the system, as it would create a lack of communication between the CESID and other services in the Ministry of Interior. Serra's fundamental interest was to prevent the CESID and the intelligence system as a whole to be allocated under the organic (and political) control of the President. In Roberto Numeriano words, “the resistance of the leaders of the Center was a sign that the military considered intelligence as a natural and strategic domain” (Numeriano, 2007, p. 17).

As a product of the reform proposals, in 2002, the National Intelligence Center (CNI) came to replace the former CESID created in 1977 with a vague legal framework and without a clear model of growth and control. The new legislation, passed in May 2002, is a reform enacting two pieces. The first one is Law 11/2002, of May 6, which regulated the National Intelligence Center. The second one is the

Organic Law 2/2002, of May 6, regulating the prior judicial control of the National Intelligence Center. By these legislations:

> The main mission of the National Intelligence Center (CNI) is to provide the Government with the information and intelligence necessary to prevent and avoid any risk or threat that affects the independence and integrity of Spain, the national interests and the stability of the rule of law and the institutions.
>
> The Center will remain attached to the Ministry of Defense.
>
> This ascription acquires a new meaning in the light of the new challenges and risks to the functions of the Center. The CNI objectives, defined by the Government, will be approved every year by the Council of Ministers and will be reflected in the Intelligence Directive (Law 11/2002, preamble).

The reform of 2002 maintained the organic dependence of the Center to the Ministry of Defense and established the core mission of protecting the country and its institutions. Like other agencies in the world, the legal reform mentions "national interests" and "integrity of the country" as broad concepts. This opened leeway enhances the state to promote its sovereign powers and defend its discretionary supremacy to define interests and preferences according to the contingency of time. Thus, those paragraphs need to be understood as directions or meta-political goals of intelligence, instead of exhaustive legislation to regulate this activity.

Law 11/2002 also defines that the National Intelligence Center needs to be subjected to parliamentary and judicial control in the terms of this and the Organic Law that regulates the prior judicial control of the National Intelligence Center. Moreover, it also determines the following functions to the Center:

> a) To obtain, evaluate, interpret and disseminate the necessary intelligence to protect and promote the political, economic, industrial, commercial and strategic interests of Spain, either within or outside the national territory;
>
> b) To prevent, detect and enable the neutralization of the activities of foreign services, groups or persons that put at risk or threat the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the State, the stability of its institutions, national economic interests and the welfare of the population;
>
> c) To promote relations of cooperation and collaboration with intelligence services from other countries or international organizations;

> d) To obtain, evaluate and interpret the traffic of signals of strategic nature, for the fulfillment of the intelligence objectives indicated to the Center;
>
> e) To coordinate the action of the different agencies of the Administration that use encryption means or procedures, guaranteeing the security of the information technologies in this area, as well as to inform about the coordinated acquisition of cryptological material and train the personnel of this and other Administrations [...];
>
> f) To ensure compliance with the regulations regarding the protection of classified information;
>
> g) To guarantee the security and protection of its own facilities, information and materials […] (Art. 2, Law 11/2002).

The points "b", "d" and "e" are of especial importance as they constitute mechanisms of surveillance deployed with the aim to protect the state and the constitutional order. Yet, the nature of the threats and the groups remain to the discretional appliance by the intelligence direction and by the Executive. The traffic of signals and cryptological materials also appear as important fronts in a digital era, especially because informational technics have replaced most of the analogical methods, such as the mentioned Janus record system. Meanwhile, the identification and methods to surveille groups have secret classification as well as the array of activities conducted by the Center. As stated in Art. 4:

> The activities of the National Intelligence Center –such as organization and internal structure, means and procedures, personnel, facilities, bases and data centers, sources of information and the information or data that may lead to know the above matters- are classified information with the degree of secrecy, in accordance with the provisions of the legislation regulating official secrets and international agreements [...] (Art. 4, Law 11/2002).

As expected, secrecy covers all the activities conducted by the Center, from sources and infrastructures to methods and intelligence flows. The Center had opened its facilities to academics and journalists in order to show a certain level of transparency and confidence to the citizens on few occasions (Matey, The development of intelligence studies in Spain, 2010). Yet, secrecy continues to be the main characteristic of this Center when compared to other public institutions. In addition, Art. 5 from the same Law determines that members of the Center will not be considered agents of authority or law enforcement officials. This point tries to avoid the politicization of the agency with police purposes; drawing a line that was crossed many times in the past during the SECED and CESID times. Yet, for the fulfillment of its functions, the National Intelligence Center may carry on security investigations on persons or entities according to the content provided in this Law and in the Organic Law for Judicial Control of the National Intelligence Center (art. 5). To carry out these investigations, the Center can obtain collaboration from

public and private organizations and institutions, even when this kind of collaboration is unknown. In that sense, monitoring certain groups or individuals can be achieved by two forms: by direct intervention over people or interception of communications by a priori judicial authorization (justifying the motives and scope of the operation); and by the implicit collaboration, in terms of resources and information, from other administrative and law enforcement institutions.

In terms of internal control, Art. 10 defines the organizational structure:

> 1. The Secretary of State and Director of the National Intelligence Center will be appointed by Royal Decree on the proposal of the Minister of Defense. The term of office shall be five years, yet the Council of Ministers might proceed with his/her replacement at any time.
>
> 2. The Secretary of State Director of the National Intelligence Center is responsible for promoting the Center's activities and coordinating the units for the achievement of the intelligence objectives set by the Government [...]:
>
> a) To prepare the proposed organic structure of the National Intelligence Center [...]
>
> b) To approve the preliminary draft budget.
>
> c) To maintain the procedures necessary for the development of the specific activities of the National Intelligence Center, as well as the conclusion of contracts and agreements with public or private entities that are necessary for the fulfillment of its purposes.
>
> d) To maintain and develop, within its scope of competences, collaboration with the information services of the State Security Forces and Police, and the organs of the Civil and Military Administration, relevant to the intelligence objectives.
>
> e) To exercise the powers granted by the legislation to the Presidents and Directors of public bodies and those attributed to them by the legislative provisions.
>
> f) To perform the functions of the National Authority of Intelligence and Counterintelligence and the direction of the National Cryptological Center.
>
> g) To perform as many other functions that are legally or regulatory appointed by the government. (Art. 10, Law 11/2002).

As observed, the legislation also sets the forms to appoint the Director of the Center and limits his/her term to avoid longer mandates and the cooptation of the center by a "permanent" director, as in the years of Emilio Manglano. Moreover, the Law established the CNI as the main node responsible for the collection and coordination of intelligence in Spain. The director should work according to government policies and restrain the activities of the Center to the mentioned functions, though, most of them are vague or open to ulterior

reinterpretations in political and legal terms. We will assess the parliamentary and judicial controls of the Center in the next sections.

Another important point is the administrative adscription of the agency. Since the CESID creation, the Center obtained organic dependency and worked for the Minister of Defense and the President of the Government. This double dependency was not symmetrical and introduced some level of disturbance because the CESID had "central" functions (intelligence assigned for the President of the Government) that were not fulfilled because the Center was a “peripheral” service with no powers to supervise other intelligence agencies in the country (Ruiz Miguel, 2005). This double dependence was modified but not extinguished in the reform of 2002. According to Law 11/2002, the President of the Government is authorized to modify, by Royal Decree, the organic adscription of the National Intelligence Center, provided in article 7.1. The Department to which the Center is assigned shall exercise the powers that this Law attributes to the Ministry of Defense. In other words, even when the Presidency wants to change the organic dependence of the CNI from the Ministry of Defense, the new institutional design should resemble the military command and the military “nature” of this activity. Thus, although the main adscription subordinated the Center to work for the Presidency, the additional amend maintained intelligence as a natural domain linked with Defense. Based on this, Royal Decree 355/2018 changed the whole adscription of the CNI from the Ministry of the Presidency back to the Ministry of Defense, simplifying the previous adscription –functional to the Presidency and organic to Defense. Thus, this change reduced the civilian oversight and emphasized the link with the military when it comes to filter information and formulate guidelines in the main intelligence node of this country.

In terms of financial control, the Second final provision of the Law establishes a vague form of budgetary supervision as it mentions that “the Ministry of Finance will make the appropriate budget modifications to ensure the provisions of this Law”. Moreover, Art. 8 from Law 11/2002 expresses that the CNI will prepare a preliminary budget each year to be approved by the Minister of Defense and the Council of Ministers. The budget should be integrated into the General State Budget from the Cortes Generales (Spanish Congress). The same article mentions that the control of the economic-financial management will be carried out in accordance with the provisions of the General Budgetary Law for Public Bodies foreseen in the tenth additional provision of Law 6/1997, of April 14, regarding the Organization and Functioning of the General State Administration. Thus, the Government establishes the necessary peculiarities that guarantee CNI autonomy and its relative functional independence. In addition, to conduct its informative activities, the CNI has an allocation of resources regulated by Law 11/95 of March 11 regarding the destination of Reserved Funds. The CNI official website mentions that the use of those funds intends to preserve identities, events, places, or dates related to activities or sources of the Center. While some states as

Brazil have created rules to mention the purposes of the funds reserved for intelligence and defense -such as the purchase of military logistics, contracts with third parties and companies- in the Spanish case, all this information appears as secret, and there is not even mention to the guidelines for this type of expenditure (Díaz-Fernández, 2013). The opacity and discretional use of these Funds, for example, was evident in the revelation of the GAL death squads during the war against ETA in the 80s. In this case, officials from the Ministry of Interior were convicted in 1998 for the appropriation of reserved funds to pay the kidnapping of a French citizen who was mistaken with a member of the Basque terrorist group (Arroyo, 1997).

To improve the economic and financial management, Royal Decree 593/2002 puts the CNI under the financial control of specific public agencies, guaranteeing adequate secrecy in the processing of the CNI documentation, and by the coordination with the General Intervention of the State Administration and the Court of Accounts. The Secretary of State Director of the CNI is responsible to edit variations of the budget and, after a prior authorization; the changes are communicated to the General Budget Office of the Ministry of Economy and Finance. The Royal Decree also specifies the internal economic procedures to turn CNI more accountable:

> The National Intelligence Center is a public agency that will produce and inform its accounts under the principles and standards of the General Public Accounting Plan and its implementing regulations. The CNI will be obliged to render accounts of its operations in the terms provided by Law 47/2003, of November 26. It might replace the documentation that could harsh classified information by a certificate of compliance with current regulations that in turn will be sent to the Court of Accounts through the General Intervention of the State Administration. The aforementioned accounts will remain deposited and under the custody of the National Intelligence Center during the legally established period. The Secretary of State Director of the National Intelligence Center, as responsible for the accounting information, will formulate the annual accounts three months before the end of the fiscal year at disposal of the Delegate Controller of the CNI for the internal audit, according to Law 47/2003, of November 26. The annual accounts, once approved by the mandatory audit of the Delegate Controller, will be safeguarded in the National Intelligence Center during a legal period. In addition, the Secretary of State Director will send a certification assuring the availability of those audits to the Court of Accounts, through the General Controller of the State Administration each year before August 1st (Accounting section, Royal Decree 1287/2005 that amends Royal Decree 593/2002).

In light of the above, the CNI is subjected to a general audit control by the rules that cover the functioning of public administration in the State. Yet, the

specificity of its sources and the preservation of classified information has an important place in this kind of control. One can see that even secrecy and sensitive materials from the agency are to be controlled by specific designs and mechanisms that respect the idiosyncrasy of the Center. Yet, accountable controls can dodge the dilemmas of transparency and secrecy by implementing an internal audit, in closed doors, that enable strict supervision of the resources and budget of the organization. Yet, this kind of restricted audience needs to avoid the mechanical and "blind" supervision of the CNI, as well as the excessive dependence on CNI to disclose budgets and internal procedures. In that sense, the National Intelligence Center is also controlled in terms of its effectiveness by the Ministry of Defense, a kind of supervision that complements the ones demanded by the General Intervention of the State Administration and the Court of Accounts in the terms of the General Budgetary Law. These kinds of control aim to verify the degree of compliance with the objectives and the proper use of the allocated resources in the agency, as well as its use to recruit new agents and establish agreements and commercial contracts within the scope of private law. Moreover, in terms of properties and contracting rules (i.e. private companies and non-state organizations), the Center is authorized to have 18% of the total credits reserved to the CNI budget at every moment. This fixed cash aims to cover periodic or repeated expenses of non-inventory material, maintenance services, and logistics.[26] Besides, the National Intelligence Center is authorized to dispose of 2.5 percent of the intelligence credits as a cash loan for the acquisition of materials and to conduct services abroad.[27]

Because of that, the budget of the agency has increased during the last years.[28] The CNI justifies this expansion "to fight radical terrorist groups and to accomplish "the control of the phenomena linked to illegal immigration, alongside the traditional terrorist threats from the domestic origin".[29] Notwithstanding, the literature is scarce in terms of assessing the financial accounts of the CNI. This issue has been partially covered by the media in cases such as the Hacking Team security leaks in 2015. This year, the Italian security company suffered a cyber-attack that revealed more than 400 gigabytes of information and data about customers that included the Spanish National Police and the National Intelligence

[26] Number 5 of article 8, Law 2/2008 of the General State Budgets.
[27] Number 6 of article 8 introduced by article 72 of Law 62/2003, December 30, regarding fiscal, administrative and social order measures.
[28] The largest amount of the CNI budget is allocated to personnel expenses (186.34 million euros), with annual increase rate of 4.1%. On the other hand, the current expenses in goods and services are endowed with 54.01 million euros and 41.27 million euros are allocated to Reserved Funds associated with the operation of intelligence services. *InfoLibre*. 'Crece el presupuesto para los espías del CNI en un 8%.' Retrieved from: https://www.infolibre.es/noticias/economia/2018/04/03/crece_presupuesto_para_los_espias_del_cni_un_81309_1011.html in 09/25/2019.
[29] The CNI's economic resources are approved annually by the Cortes Generales through the successive General Budget Laws of the State. See economic allocation in: https://www.cni.es/es/queescni/quees/, accessed in 09/25/2019.

Center (CNI). The company has always been surrounded by controversy, with accusations of illegal support to dictatorships and sales of surveillance programs to access files from computers and mobile phones of dissidents.[30] The CNI appears in a contract held from 2010 to 2016 in which the company was paid 3.4 million euros. At that time, the CNI recognized that it hired the company, but the agency denied any link with illegal or unethical activities. Furthermore, the Center reinforced the idea through which intelligence contracts are always conducted "following the laws of the public sector and the administration."[31]

In terms of ethical protocols, the National Intelligence Center created several principles and rules that are to be adopted by its practitioners. In a manual released on the official website, the center affirms its commitment as an institution to the "service of Spain and Spaniards, guaranteeing security, protection and promoting the national interests." This fundamental principle "defines the essence of the organization, inspires its activities, and governs the performance of all its members."[32] Furthermore, the CNI officially emphasize the importance of these principles: rectitude in the fulfillment of duty, spirit of sacrifice, the reserve of information, objectivity and impartiality (to make analysis, judgments, and values), dedication and effort, assumption of responsibilities, companionship, authority and leadership (authority in a fair and balanced way), training (acquisition of deep technical capacity), honesty (integrity and dignity), and defending the reputation of the Center. It is not our objective to analyze the professionalization of intelligence in Spain. Yet, the mentioned values and ethical principles serve to depict a series of concepts that each agent and analyst should consider to restrain intelligence itself and promote social values in the accomplishment of CNI missions and tasks. That is, by expressing those values, the Center tries to show some degree of responsibility for the use of special procedures allowed by law. Thus, the Center should adopt proportionality in its actions, balancing the magnitude of potential risks or threats and the collateral effects to obtain sensitive and strategic knowledge from different sources. Finally, the ethical Decalogue also expresses traditional values that are common to security and military organizations, such as a "sense of commitment, discretion, the spirit of sacrifice, loyalty, respect for colleagues and subordinates, teamwork, high-mindedness and the pursuit of excellence."[33]

---

[30] Marquis-Boire, M.; Scott-Railton, J.; Guarnieri, C. 2014, June 14th. 'Police Story Hacking Team's Government Surveillance Malware.' *The Citizen Lab*. Retrieved from: https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/ in 09/27/2019.

[31] Cano, R. J. 2015, July 7, La policía y el CNI, entre los clientes de una firma de 'hackers', *El País*. Retrieved from: https://elpais.com/politica/2015/07/07/actualidad/1436284983_731864.html in 09/27/2019.

[32] Ap. in CNI official website: https://www.cni.es/es/, consulted in 09/30/2019.

[33] Idem

In the case of Spain, Intelligence Policy or Plans are not published. Yet, the Center has the mission to work following the Directive of Intelligence approved each year by the Government. The Directive is formulated by the CNI and proposes the annual objectives of the services, and those to be integrated into the "Annual Intelligence Directive" to the President of the Government. This Directive addresses the tasks and intelligence efforts in coordination with the State Security Forces and the Police. In the Spanish intelligence community, the CNI has a central position to provide the Government with valuable information (*see Figure 9*). According to its official website, the Center is working to improve gathering capacities and the internal and external deployment of agents, especially in areas of conflict in the Middle East and the Maghreb. Moreover, the Center supports operations that the Spanish Armed Forces develop in other countries, as in the case of international cooperation in the military affairs of NATO. The official website also mentions that the main sources of information to the Center are human sources (HUMINT). Meanwhile, this information is contrasted with other technical means (SIGINT/IMINT/FININT/etc) and with the information provided by foreign services. Information from open sources (OSINT) is also valuable but on a lesser scale.

Finally, the CNI has a Counterterrorism Division that works both at national and international levels to detect and mitigate potential terrorist threats, although the definition of terrorism does not point, a priori, to criminal law or international treaties. In that sense, CNI participates in the Intelligence Center for Counter-Terrorism and Organized Crime (CITCO) through the integration of personnel assigned to work with Security and Police Enforcement agencies since 2014. The CITCO works according to the intelligence tasks assigned by the Government to elaborate reports on terrorism. These reports are a product from the analysis of information and operational methods related to organized crime and violent radicalism that are relevant or necessary for the development of strategic and prospective criminal intelligence concerning these phenomena. The CITCO mission consists also of establishing the coordination and action of the Operational units of the State Security Forces and Police Corps.[34] This coordination is to be promoted in a permanent base and developed under specific competencies that the different provisions and agreements, both national and international, entrust to the Ministry of the Interior in order to fight terrorism and organized crime. Since 2018, CITCO also has access to National Passenger Records to make a cross-reference analysis of passengers' data with Law Enforcement and Intelligence systems to detect potential targets and prosecute suspects according to 26 different criminal offenses. The system is capable of automatically log the information sent by air carriers and can create profiles according to predetermined characteristics, for instance: woman, 30 years old, traveling to Turkey, French national. The program

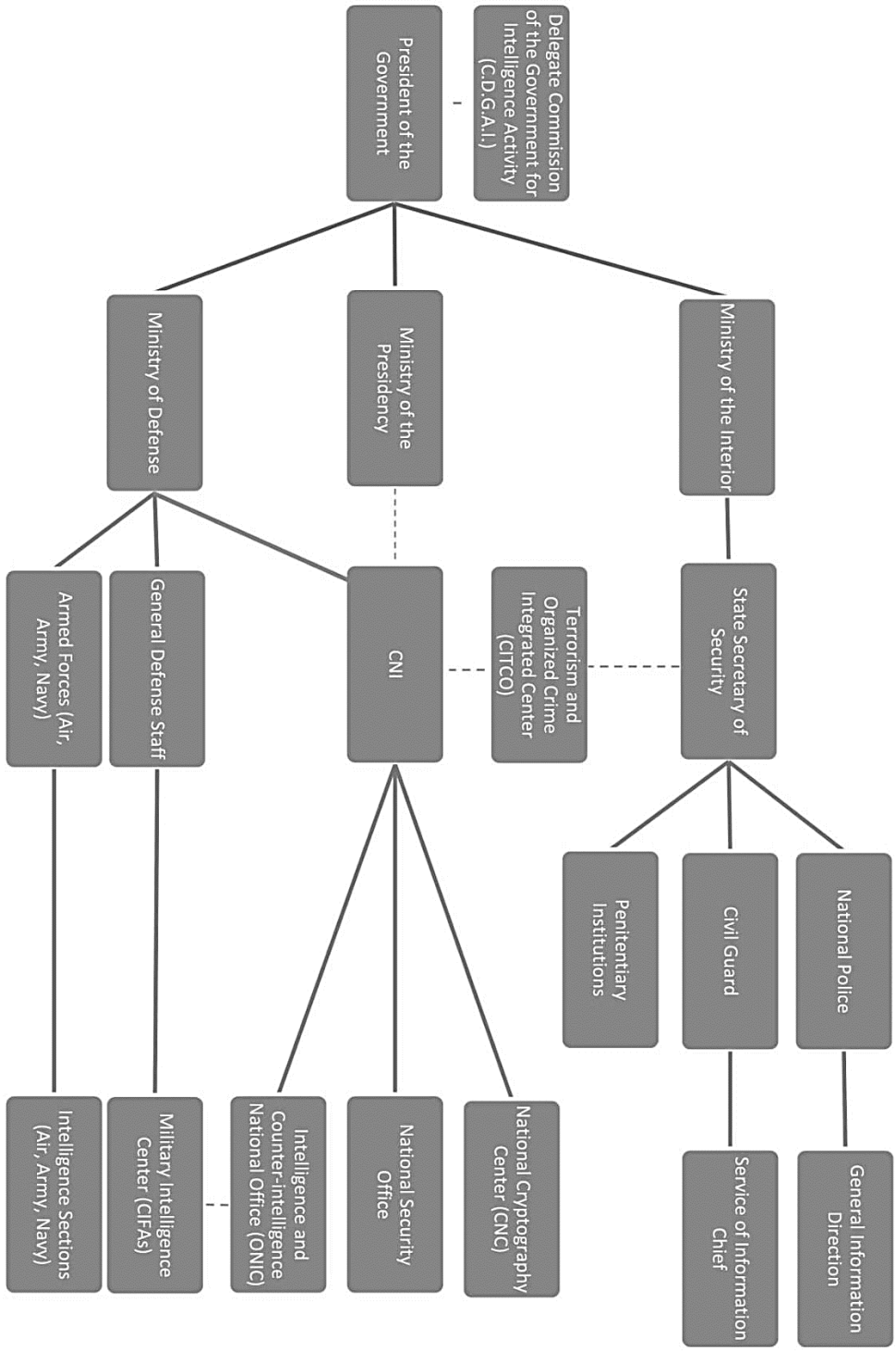
[34] See Royal Decree 873/2014, of October 10, that modifies the Royal Decree 400/2012, of 17 of February regarding the basic organic structure of the Ministry of the Interior.

has been criticized because of the controversial proportionality and lack of external control. However, it has been supported by security and enforcement agencies especially after the terrorist attacks in London, Nice, Paris, and Barcelona during the last years.[35]

Figure 9 shows the network and institutions that cooperate with the National Intelligence Center (CNI) constituting the Spanish intelligence community. The dotted line indicates the functional connections or intelligence cooperation while the full lines indicate the administrative and hierarchical dependence among the referred institutions. One of the pillars of the Spanish intelligence community is the "Delegate Commission of the Government for Intelligence Affairs", which ensures the adequate coordination of all information of the state for the coordination of the intelligence community. Until 2018, it was chaired by the Vice President of the Government designated by the President and composed by the Ministers of Foreign Affairs, Defense, Interior, and Economy, as well as the Secretary-General of the Presidency, the Secretary of State for Security and the Secretary of State Director of the Center National Intelligence, who acted as Secretary. The Delegated Commission of Intelligence has the following functions: a) To propose the President of the Government the annual objectives of the CNI that must integrate the Directive of Intelligence; b) Monitoring and assessing the development of the objectives of the CNI; c) To ensure the coordination of the CNI with the information services of the State Security Forces and Police Corps (i.e. National Police and Civilian Guard), and the organs of the civil and military administration (Law 11/2002, Art. 6). As the Commission has reserved and classified characteristics, a deep assessment of its activities is still required.

[35] Dolz, P. O. 2018, January 23. 'Spain to cross-reference passenger flight information with police databases.' *El País*. Retrieved from: https://english.elpais.com/elpais/2018/01/23/inenglish/1516708352_265986.html in 09/30/2019.

Figure 9: The Spanish intelligence community and the CNI (at state level)



Source: the author

In Brazil, after the Coup d'état in April 1964, the military approved Law 4.341 to create the National Service of Information (SNI). The SNI was created to orient and coordinate the information and counter-information activities related to the Public Administration in the three federative levels (Union, States, and Municipal administrations), to support the decisions of the President of the Republic and the National Security Council. The SNI was subordinated to the Presidency of the Republic and the Federal Senate appointed the Chief of the Service. However, the senators were indirectly indicated by the military as they imposed a bi-partisan system. Decree 60.417, of 1967, expanded the Service beyond the Central Agency and created twelve regional agencies distributed across the national territory.

In addition, the SNI was responsible for coordinating the National Information System (SISNI), implementing the National Information Plan (PNI) based on the National Security Doctrine. Years later, Decree 68.448 of 31/3/1971 created the National School of Information (ESNI). Meanwhile, these offices or departments comprised the SNI: Political, economic, ideological, psychosocial, administrative, and security of information. In parallel, there were information agencies subordinated or linked with other ministries, such as state companies and municipalities that collected information to the central agency. Institutions as diverse as the Bank of Brazil, the Health Foundation Oswaldo Cruz, Mining Company *Vale do Rio Doce*, and The National Library had their activities monitored by informants working for the sake of "national security". In that sense, it is important to note that the SNI was not a politically neutral body designed to inform the president. The Service acted as a stealthy "political advisor" that offered information to the President in several issues, such as surveilling other militaries and monitoring civilians in the federal Congress (Gaspari, 2014).

After the military regime, the Federal Constitution of 1988 accelerated the transition process to a democratic regime. This year, the General Secretariat of the National Security Council became the National Defense Advisory Board (SADEN). The Constitution also extinguished the National Security Council - which existed since 1934 and advised the presidents during the dictatorial regime – and replaced by the National Defense Council. In this change, the Council was redirected to external defensive tasks, without any mention to the National Security Doctrine as in the Constitution of 1967 (Carpentieri, 2016). Moreover, Article 144 of the Constitution of 1988 abolished the CODI-DOIs system and redirected its tasks to the Federal Police. However, in those changes, personnel and doctrines were simply renamed and reallocated in the new organizations. It must not be a surprise, for example, that the Federal Police, headed by Deputy Romeu Tuma, former director of the Department of Political and Social Order (DOPS) of São

Paulo, commanded parallel police within this institution to surveille target groups according to his personals interests (Brandao, 2019).

As mentioned, the SNI was not reformed during the formulation of the new Constitution. Although the Service intended to improve its image to the public, "the organization monitored labor strikes that occurred in the late 80s, especially the ones related to land reform in rural areas" (Hunter, 1997, p. 55). Years later, President Collor de Mello abolished the SNI by the Act 150/1990 (Law 8,028/1990). The decision to extinguish the SNI has never been clarified. At that time, the Act was understood as personal revenge of Collor since the service released a dossier to undermine his presidential campaign. The extinction of the SNI can be interpreted as a radical form of internal control promoted by the Executive, a self-restraining action stemmed by the Presidency itself. Because of this, the SNI functions were transferred to the Secretariat for Strategic Affairs (SAE) of the Presidency of the Republic. However, the SAE was the continuation of the SNI insofar as it maintained the same personnel and organizational structure. For example, "former SNI agents were still working with the new generation of analysts when the Brazilian Intelligence Agency (ABIN) was created ten years later" (Gonçalves, 2008, p. 511).

During the 90s, between the official ending of the SNI and the creation of the ABIN in 1999, there were not substantial regulations in the realm of intelligence. Firstly, because the SAE absorbed the technical apparatus and the intelligence actions of the SNI. Secondly, because the Executive used Provisional Acts to block the work of the Congress. During Fernando Henrique Cardoso Presidency, the Executive bargained the proposals to create a new intelligence service, tailoring legislative proposals according to its preferences and blocking those formulated by Congressmen from opposed parties (Antunes, 2002). These negotiations took more than five years and concluded with two administrative reformulations: the creation of the Cabinet for Institutional Security (GSI), and the creation of the Brazilian National Agency (ABIN) within the Brazilian Intelligence System (SISBIN).

Law 9.883/1999 enacted the ABIN and the Brazilian Intelligence System (SISBIN) in a short text of 15 articles to establish the purposes and the main ground to consolidate a new intelligence community. In the text, the SISBIN was to integrate the planning and execution of the country's intelligence activities, to provide support to the President of the Republic in matters of national interest (art. 1). As an attempt to erase the explicit mention to the National Security Doctrine, the SISBIN missions were converted to preserve "the national sovereignty, the defense of the Democratic State of Law and the dignity of human beings" (art. 1). The Law also mentions "respect and preserving the individual rights and guarantees and other provisions of the Federal Constitution […]" (art. 1). According to the Law:

> […] intelligence is understood as the activity that aims to obtain, analyze and disseminate knowledge inside and outside the national territory about facts and situations of immediate or potential influence on the decision-making and governmental action. Intelligence should safeguard the security of society and the State; […] counterintelligence is understood as the activity that aims to neutralize adverse intelligence (Art. 1, Law 9.883/1999).

The legal definition above reminds the theoretical definition of intelligence as a process and as a form of knowledge (see section 3.1). Intelligence, in that sense, is a specific process to obtain and refine information to high policymakers and guarantee the security of the socio-political order. The legal text also mentions that other entities of the Federal Public Administration can also produce intelligence knowledge, especially those related to external defense, internal security, and foreign relations. Those institutions constitute the Brazilian System of Intelligence (SISBIN), in the forms established by the President of the Republic. The SISBIN is responsible for obtaining, analyzing, and disseminating information necessary for "the decision-making process of the Executive Branch, as well as for safeguarding the information against unauthorized persons or groups" (art.2). As the SISBIN is a network, the ABIN is the central agency or the main node within the System. In that sense, the ABIN should plan, execute, coordinate, supervise, and control the intelligence activities in the whole system (See Acts 999-17 of 2000 and 2,216-37 of 2001).

According to the legislation, the ABIN and the SISBIN activities are developed under secret techniques and means. However, those activities should be conducted in accordance with "individual rights and guarantees, fidelity to the institutions and ethical principles that govern the interests and security of the State" (art. 3). Moreover, the ABIN is responsible for evaluating the internal and external threats to the constitutional order; as well as of promoting the development of human resources and the doctrine of intelligence, through studies and research for the execution and improvement of intelligence activities (art. 4). In that sense, the execution of the National Intelligence Policy, established by the President of the Republic, is coordinated by the ABIN under the supervision of the Chamber of Foreign Relations and the National Defense of the Governing Council. The National Intelligence Policy was only developed in 2009 after consultation and approval of the Congress. In addition, However, the President of the Republic has the choice to nominate the Director-General of the ABIN, after approval by the Federal Senate (art. 11). We will return to the legislative control of intelligence in the next section.

As Law 9.883/1999 only created the basic ground to constitute the new intelligence agency and system, new legislation was necessary to fill the gaps in this realm. Hence, Decree 4.376/2002 enacted further rules for the organization

and functioning of the Brazilian Intelligence System. In that sense, it mentioned that

> Art. 2 For this Decree, intelligence is understood as the activity for obtaining and analyzing data and information to produce and disseminate knowledge, within and outside the national territory, concerning facts and situations of immediate or potential influence over the decision-making process, the governmental action, the safeguard and the security of the society and the State.
>
> Article 3 - Counterintelligence is understood as the activity that aims to prevent, detect, obstruct and neutralize adverse intelligence actions of any nature that constitute a threat to the safeguarding of data, information, and knowledge of interest to the security of society and the State.

Furthermore, Decree 4.376/2002 expresses that the SISBIN comprises the following bodies: I. The Civil House of the Presidency of the Republic, through its Executive Secretariat; II. The Secretariat of Government of the Presidency of the Republic, by the coordinating agency of federal intelligence activities; III. The Brazilian Intelligence Agency - ABIN, via the Office of Institutional Security of the Presidency of the Republic, as the central organ of the System; IV. The Ministry of Justice, through the Federal Police Department, the Federal Traffic Police Department, and the National Penitentiary Department [...]; V. the Ministry of Defense; VI. The Ministry of Foreign Affairs; VII. The Ministry of Finance; VIII. The Ministry of Labor and Social Security; IX. The Ministry of Health; X. The Military House of the Presidency of the Republic; XI. The Ministry of Science and Technology; XII. The Ministry of the Environment; XIII. The Ministry of National Integration, through the National Secretariat of Civil Defense; XIV. The Accounting-General Office of the Union; XV. The Ministry of Agriculture; XVI. The Civilian Aviation Secretariat of the Presidency; XVII. The Ministry of Transport; XVIII. The Ministry of Mines and Energy; XIX. The Ministry of Communications, through its Executive Secretariat.

The broad extension of the SISBIN resembles the creation of a superstructure to integrate and produce intelligence in the country, as in the sense of a giant bureaucratic apparatus in the model of the previous SNI. In the current System, those organizations are to produce knowledge in compliance with the prescriptions from the National Intelligence Policy, exchanging information for the production of knowledge related to intelligence and counterintelligence activities, and providing the central body (the ABIN) with information and knowledge related to the defense of national institutions and interests (Art. 6). To inculcate the integration and cooperation among the many organizations of the System, the "Consultative Council of the Brazilian Intelligence System", attached to the Secretariat of State of the Presidency was created to propose the general norms and procedures for the exchange of knowledge and communication within the SISBIN (art. 7). The Secretariat of Government, the Brazilian Intelligence Agency,

the Federal Police, the Armed Forces, the Financial Ministry, and the Foreign Relations Ministry integrate the Council. The Council is headed by the Secretariat of Government of the Presidency of the Republic (Art. 8). The Council meets in an ordinary base (up to three times per year) at the ABIN headquarters in Brasília or according to the discretional demands of its members. *Figure 10* shows that the SISBIN is comprised of many organizations that can be divided into three branches: Public Security Intelligence Subsystem – SISP (right branch in the figure), Strategic Intelligence Subsystem – coordinated by ABIN (medium branch), and Defense Intelligence Subsystem (left branch in the figure). The figure also shows the main council bodies attached to the Presidency of the Republic and the different institutions in the three branches. The full lines show the administrative hierarchies and dependencies, whereas dotted lines depict the functional connections between the mains organizations of the SISBIN. In this system, the ABIN performs a central function as the main node of intelligence coordination.

From the technical point of view, the legal concepts adopted in the SISBIN system are aligned to contemporary legal structures of democracies around the world. Yet, if the Spanish CNI has similar duties, like to coordinate the strategic intelligence and to establish a link with security agencies, the Spanish Law is not as extensive as the Brazilian one to regulate the forms of that cooperation. The ABIN, in turn, is responsible for managing and coordinating a constellation of organizations that never had worked together. That is, if the parts of the SISBIN are obliged to provide the ABIN with specific data and knowledge related to the defense of national institutions and interests, the forms to report and synchronize the data in the System are still not clear. For example, it remains unclear the role of the ABIN in relation to the intelligence made by other organizations, such as the intelligence disseminated by the Federal Police or by the Civil Police in each federal state. Therefore, to incorporate other organizations to the federal sphere, it was necessary to create the Public Security Intelligence Subsystem through Decree No. 3,695/2000. However, even with the creation of intelligence subsystems in the SISBIN, it is still not clear how the ABIN would exercise operational control over other institutions. For example, the SISBIN coordination and data exchange depends also on friendly relations between different bureaucracies. In other words, the organizational forms and hierarchies between the array of institutions, aside from a general direction and coordination by the ABIN, are still an ongoing process.[36] Moreover, it is still unclear to whom the system will respond in cases of failure, deviation of power, and inefficiency beyond the ABIN accountability

[36] Another initiative to foster the integration of the System was the creation of the Advisory Council of SISBIN. This body is formed by the heads of the Institutional Security Office and ABIN. In the scope of the Ministry of Justice, by the leaders of the National Secretariat of Public Security (SENASP), the Police Intelligence Directorate of the Federal Police Department and the Federal Highway Police Department. There is also participation of the military intelligence agencies, linked to the Ministry of Defense, the members of the Financial Activities Control Council of the Ministry of Finance (COAF), and the General Coordination to Combat Transnational Illicit Trafficking and the Ministry of Foreign Affairs.

actions before legislative bodies. Nonetheless, one should observe that Decree 4,376/2002 shows a concern to respect the administrative leeway of each organization and preserves their relative autonomy in the federative system.

To mitigate the problems of coordination, the Administrative Act of March 25, 2009, established the Integration Center of the Brazilian System of Intelligence (CINTEG/SISBIN). As the name suggests, is creates standards for the integration in the System being supported by the ABIN, which grants security and secret credentials to the members of the Center. The Act also mentions that the exchange of data and knowledge within the CINTEG/SISBIN will result from the formal request or initiative from each organization in the system (art. 7). Besides, information and knowledge in the system will be stored in a Database of this Center through the terms of restricted access and consultation (art. 7.1 and 7.2). Therefore, the Center aims to improve the data integration and coordination of the System. Yet, in the recent governments, the arrangement and nominations of Ministries have changed according to the circumstances and preferences of the Executive, turning this integration dependent on the own institutional designs and initiatives of the Ministries.[37] *Figure Y* shows the complete institutional configuration of the Brazilian Intelligence System (SISBIN) as defined by the above norms.

As shown in figure 10, the SISBIN is integrated by specific subsystems: the Public Security Intelligence Subsystem (SISP) and the Defense Intelligence Subsystem (SINDE). The first subsystem, the SISP, was regulated by the National Public Security Secretariat through Resolution No. 1/2009. In practice, the SISP has become the second intelligence system at the federal level, parallel to the one coordinated by the ABIN.[38] The SISP is coordinated by the National Secretariat of Public Security (SENASP) of the Ministry of Justice and the main operational components are the Federal Police Department (DPF), the Federal Traffic Police Department (DPRF), the Ministry of Justice, and the Financial Activities Control Council (COAF), among other organizations located in other levels of the federation. Because of the constellation of organizations, some authors suggested that this subsystem integrates the SISBIN only partially or incompletely (Cepik & Möller, 2017). The second subsystem, the SINDE, is coordinated by the Department of Strategic Intelligence (DIE) of the Ministry of Defense. The SINDE articulates this ministry with intelligence centers from the Armed Forces (Navy, Army, and

[37] For example, Decree Nº 8.149, 2013 amends Decree No. 4,376, 2002, which regulates the organization and operation of the Brazilian Intelligence System, updating the names of the ministries in the System.

[38] In addition to the Special Subsystem Council, the SISP is comprised by the National Network of Public Security Intelligence (RENISP), the National Network for the Integration of Public Security, Justice and Surveillance Information (INFOSEG), which currently interconnects the databases (SINIVEM)), and contains information on police investigations, criminal prosecutions, firearms, vehicles, drivers licenses and arrest warrants, and the National System for the Identification of Vehicles in Motion (SINIVEM). See figure 10.

Aeronautics) and the Highest Defense General Staff. The Ministry of Defense coordinates the intelligence services of each Armed Force.

Explained the institutional design, let us consider the performance and functions of the SISBIN. In that sense, Decree No. 8.793 of 2016 was important as it established the first National Intelligence Policy (PNI). According to the Decree, intelligence activity still aims to produce and disseminate "knowledge to the competent authorities, regarding facts and situations occurring inside and outside the national territory, to influence the decision-making process, to governmental action, and to safeguard society and the state". Again, the federal definition of intelligence is too broad and is capable of encompassing every situation for the sake of "society and the state". Yet, the state must restrain itself insofar as the intelligence activity must be based on respect to the "Fundamental Principles, Rights and Guarantees expressed in the Federal Constitution, in favor of the common good and defense of the democratic rule of law". In that sense, the Policy clarifies many assumptions of the intelligence activity, such as

> State Activity Intelligence is an exclusive activity of the State and is an instrument to advise the highest level of successive governments, in what concerns the interests of Brazilian society. It must attend the State in the first place, not putting itself at the service of groups, ideologies, and objectives that are changeable and subjected to political-partisan conjunctures.
>
> [...] State Intelligence should monitor and evaluate the internal and external conjunctures, seeking to identify facts or situations that may result in threats or risks to the interests of society and the State. The work of Intelligence must enable the State to mobilize the necessary efforts to cope with future adversities and to identify opportunities for governmental action.
>
> [...] Permanent Intelligence is a perennial activity and its existence is attached to the State it serves. The need to advise the decision-making process and to safeguard the nation's strategic interests are dictated by the State in situations of peace, conflict, and war.

According to the lines above, the Policy (PNI) urges to disassociate intelligence activity from a "government policy" understood as the particular choices of Presidents. This means that intelligence aims to support the choices of the Executive as a state, instead of serving the government ideologies and partisan options. However, the process of choosing guidelines and strategic objectives for the state cannot be separated from a political context, since those are political choices themselves. Moreover, intelligence for the state cannot be politically neutral, as the state cannot be fully separated from the government. In that sense, intelligence, as a bureaucratic activity, has limits and restrictions imposed by the authority of the President as he mediates the legitimacy of the people and sets the principals to command the administration. As the PNI aims to renounce to President impositions for the sake of the state, the text creates a dissonance in

relation to other contemporary systems of intelligence. In contemporary systems, the ruler of the Executive is the one who imposes the intelligence strategy for the subordinated organization. The intelligence staff, as state bureaucracy, should support the authority of the Executive, instead of avoiding its command or capturing its power.

Carpentieri (2016) affirms that the 'Policy' resonates with the National Security Doctrine. To him, the PNI insists on respecting democratic institutions and fundamental guarantees while it preserves concepts that refer to the military notion of internal defense as in the authoritarian period. The deliberate opposition to new threats represented by "interest groups, organizations or individuals acting adversely to national strategic interests" resembles the doctrine of the Higher School of War in the times of the military governments. This is because those interests and groups can easily justify monitoring social movements, public associations, universities, labor unions, and other "suspecting groups" by item 2.2. According to the PNI, the role of intelligence is "to monitor and evaluate the internal and external conjunctures, seeking to identify facts or situations that may result in threats or risks to the interests of society and the state" (Introduction, Decree 8.793/2016). Indeed, when the ABIN director, General Alberto Cardoso, explained to the National Congress in 2002 the need for intelligence based on state policy (rather than on government policy), such a doctrine blurs the line of possibilities, allowing to surveille every social actor if the interpretation falls under "the dangerous potential to destabilize the country" (Antunes, 2002, p. 150). In that sense, the PNI expresses that the organizational aspects attached to the intelligence community define the scope and instruments of intelligence. In other words, intelligence supposedly is what intelligence agencies do, rescuing a self-referential and hermetic paradigm for this activity.[39]

Furthermore, the PNI defines the following phenomena as threats to the country:

> […] espionage, sabotage, external interference, actions against national sovereignty, cyber-attacks, terrorism, weapons of mass destruction (nuclear weapons), organized crime, corruption (demanding a better cooperation with other agencies to restrain this phenomenon), actions that contradict the democratic Rule of law (those actions that violate the federative pact, fundamental rights and guarantees, the dignity of human beings, the welfare and health of people, political pluralism,

[39] The essential instruments of the national Intelligence are self-referential, such as: I – the National Policy of Intelligence; II – the National Intelligence Doctrine; III – the directives and priorities established by the competent authorities; IV - SISBIN and its intelligence branches; V – the exchange of data and knowledge within the SISBIN, in accordance with the legislation; VI – the integrated plan for the cooperation system between SISBIN member bodies; VII - the training and development of people for the Intelligence activity; VIII – the research and technological development for the fields of Intelligence and Counterintelligence (Decree 8.793/2016).

environment and critical infrastructures, and the constitutional precepts related to the integrity of the State) (Section 6, Decree 8.793/2016).

The list of the above phenomena is the main path in which intelligence should direct its missions and constitute a state policy. As seen, the array of threats, since nuclear weapons to corruption and defense of the population, serve as the ground upon which intelligence stands and promotes itself as a sovereign power to rule and redefine the political life of the country. Intelligence is not political police, but it arises as a privileged area just by the fact of containing a plethora of threats (some of them are concrete ones, while other ones are catchall concepts). This becomes clear when the PNI expresses that the objectives of the National Intelligence are the promotion of security and the interests of the state and Brazilian society.

Because of that, we can express that the intelligence services and policymakers ignore the differentiation between the security of the state and security of populations, subsuming the latter to the former, and expressing, with no restrictions, that a situation of security to the state is as important and corresponds automatically with a situation of security to the population. In this scenario, intelligence develops the capacity to advise policy-makers through tools, structures, and processes that enable such identification in the various areas of "national interest". However, this is an interest defined from above; a realm in which the guiding mechanisms are the preservation of the state and the political order *as a whole*. In that sense, this order must prevail over the heterogeneity of groups in the population, the menaces stemmed from below, as well as the threats from other states and international groups. In that realistic logic, if the state is concerned about menaces everywhere, it should be able to declare sovereign powers to combat those threats in a delicate equilibrium between top-down surveillance that identifies and monitors menaces, and the necessity to restrain the impetus to securitize everything and everybody who has the "potential" to alter the "national" interests.

The idea of sovereign power rescues the importance of setting controls to redefine and restrain activities such as intelligence. In light of that, in terms of financial control, there are different mechanisms to regulate the expenditures and budgets of the ABIN. For example, the "Relatórios de Gestao" (Management Reports) redacted by the Agency each year on the official website show some clues about this kind of control. The Management Report of 2008 accounts for the internal structure of the Institutional Security Cabinet (GSI), and the administrative tasks that have been executed (seminars, logistics, budgets, as well as national security and public safety objectives) in the Agency. However, the report is generic in the description of those objectives and lacks evaluation of the money spent on the administrative tasks. Moreover, in 2008, the Secretary of Planning, Budget, and Administration of the ABIN refused to provide data to the

Office of Internal Control of the Presidency of the Republic. The accounts of 11.5 million reais used in corporate cards were not accepted and sent to the Federal Court of Audits for verification (Carpentieri, 2016). The ABIN Secretary justified the refusal to provide details of the expenditures on the grounds of secrecy. However, the Federal Court of Audits (TCU) found irregular expenditures that should have been declassified, such as restaurant bills and the purchase of televisions and luxury cars. In that year, a joint National Congress commission investigated government expenditures on corporate cards by the ABIN.[40] In the Commission reports, the development and growth of the Agency over the last years became evident. For example, the agency's budget was R$ 124.5 million in 2003, while it increased to R$ 327 million in 2009, R$ 527.7 million in 2012, R$ 515.2 million in 2014, and R$ 611.7 million in 2017. Important to notice that about ninety percent of the expenses during that period were used in human resources and staff.[41]

In order to show a certain level of transparency, the ABIN started to improve the Management Reports in the last years. For example, the Report of 2017 was written in accordance with the rules of the Federal Court of Audits (TCU), which regulates the annual expenditures in the Federal Public Administration, providing information and statements on the Brazilian Intelligence Agency (ABIN). The document included the following topics: ABIN overview; organizational planning and results; governance, risk management, and internal controls; special areas of management; relationship with society; financial performance and accounting information; management compliance, and control demands. The extensive Report recommended accountability measures such as integrity to inform the ABIN contracts, as well as integrity and completeness to redact files to the System of Appreciation and Registration of Acts of Admission and Concessions (SISAC). Moreover, the Report also expressed that the ABIN needed to comply with Law No. 8,730 of November 10, 1993, regarding the declarations of assets and incomes; demanding more reliability to store accounting records in the Integrated System of the Financial Administration (SIAFI).

The improvement of the relationship between the ABIN and the TCU can be explained because the latter is also part of the SISBIN, helping the intelligence agency to identify threats to the state in terms of money laundering, organized crime, and corruption. Since the SISBIN integration depends on the good relationships between ABIN and other federal organizations, the former needs to

[40] Odilla, F. 2008, July 28. 'Abin se recusa a detalhar seus gastos à Presidência da República.' *Dourado News*, retrieved from: https://www.douradosnews.com.br/noticias/abin-se-recusa-a-detalhar-seus-gastos-a-presidencia-da-republica-86b37/335959/ in 10/02/2019. See Goncalves,, Joanisval Brito. 'Políticos e Espiões – O controle da atividade de inteligência'. Niterói: Impetus, 2010, p. 173.

[41] See the ABIN Management Reports in: http://www.abin.gov.br/acesso-a-informacao/auditorias/, consulted in 10/02/2019.

show synchronization with the TCU accounting system if it wants back information that might help the service to create financial intelligence products.

Another internal control mechanism is the Inspections Office (*Corregedoria Geral* - COGER), subordinated to the ABIN Director. Based on Decree No. 8.905/2016, the COGER is responsible for investigating irregularities and disciplinary infractions committed by ABIN public officials. It is not clear if the model of this agency is performed according to the inspection model from Anglo-Saxon countries, in which the inspector has autonomy and is independent of the intelligence services. To be more precise, the mandates, composition, and appointment of the COGER might be similar to the Police *Corregedorias*, which are Brazilian administrative figures that depend on the internal command of police Chiefs to investigate deviations of power and corruption within those organizations.

The ABIN also implemented *Ouvidorias Gerais*, a sort of Ombudsman or body for control and social participation. However, ABIN *Ouvidoria* is part of the structure of the Office of the Director-General. It has the mission to receive complaints, requests, suggestions, and compliments related to organizational procedures in order to improve the management within the agency. This Ombudsman's Office is a regimentally administrative structure with the mission to communicate the public and the internal staff with the ABIN Director. The ABIN Director is also supported by the Internal Control Advisor (ACI) board, who is responsible for: a) Guiding the management of public assets and resources following the recommendations of the TCU; b) Promoting initiatives and good practices in administrative acts; and c) Updating norms and guidelines regarding the programs, doctrines, and actions of intelligence.

The ABIN Management Report from 2017 also mentions details about the financial expenditures related to paper, desk materials, and even coffee. Although the agency does not mention the exact expenditures, it shows those issues to ensemble deep transparency, like many other organizations that have incorporated New Public Management principles. The report also mentions the agency budget related to generic programs, sub-departments, and objectives (such as technology acquisition, planning of counter-terrorism actions, planning actions within institutional frameworks, improving links with foreign services, and so on). Hence, the report might be a good example to show a certain degree of transparency without compromising the secrecy of concrete sources and operations.

The above administrative and financial controls are positive points that always should be improved. However, since they are elaborated to account for the internal procedures, one must be skeptical about their promises and capacities to control the ABIN. For example, *Corregedorias* and *Ouvidorias* lack administrative

independence to process complaints and correct internal deviations. Another important obstacle to a more efficient ABIN internal control is the controversial subordination of the Agency to the Institutional Security Cabinet (GSI), which works as an intermediate organization between the President of the Republic and the intelligence service. Let us introduce a brief evolution and the main effects of this subordination.

Provisional Measure 1.911-10/1999 enacted the GSI as a Government Ministry based on Amends presented by the former Representative Jair Bolsonaro. The GSI is an office that stemmed from the traditional functions of the previous Military House (that ensured the safety of the President and his/her family), and is responsible to manage critical situations for the Executive as well as to to the institutional stability of the country. In that sense, the GSI was enacted to command the ABIN and the National Anti-Drug Secretariat, showing that intelligence and criminal enforcement are closely related in the Post-Cold War scenario. The GSI gained power during the administration of presidents Fernando Henrique Cardoso (1996-2002) and Luís Inácio Lula da Silva (2003-2010). Since those years, the GSI Chief is a high military appointed by the President of the Republic to supervise the ABIN General Director, whose nomination must be approved by Congress. This institutional arrangement subordinates the main agency of the civilian intelligence system – the ABIN – under the command of a military organization ruled by the Armed Forces. The GIS acts like an intermediate player between the President and the ABIN, commanding the intelligence service. In other words, the ABIN lacks a direct contact or channel with the president of the country.

Therefore, despite the ABIN legal mandates to command the Brazilian Intelligence System, in practice, the agency is subordinated to the GSI interests. The ABIN performance and accountability depend on the supervision and actions of the GSI leaders; as well as in the bargains of power between the Military and Diplomats over strategic intelligence (Arturi & Rodriguez, 2011). Because of this administrative subordination, on the one hand, the ABIN should coordinate the SISBIN and disseminate intelligence amidst the "chaos" of interests and administrative routines from other public security and defense organizations (*see Figure 9*). On the other hand, the mentioned military body (the GSI) filters the synchrony of this action, which should go to the center of the Executive Branch, i.e. the Presidency of the Republic.

In light of that, the leader of the Executive has a double alienation. Firstly, the National Intelligence Police seeks to establish a "state" intelligence that is independent of those who are in charge of the government by virtue of elections. Secondly, the supremacy of a military minister, the GSI Chief, allows control over the flow of information that originally should reach the President. This means that military bureaucracy filters and disseminates strategic intelligence over and from

the ABIN. In that sense, the GSI might operate as a super-ministry managing the crucial information related to defense and security. The GSI became extinct during the ministerial reform promoted by the government of Dilma Rousseff in October 2015, but as soon as the Chamber of Deputies removed her in the impeachment process, the interim president Michel Temer reactivated the GSI.

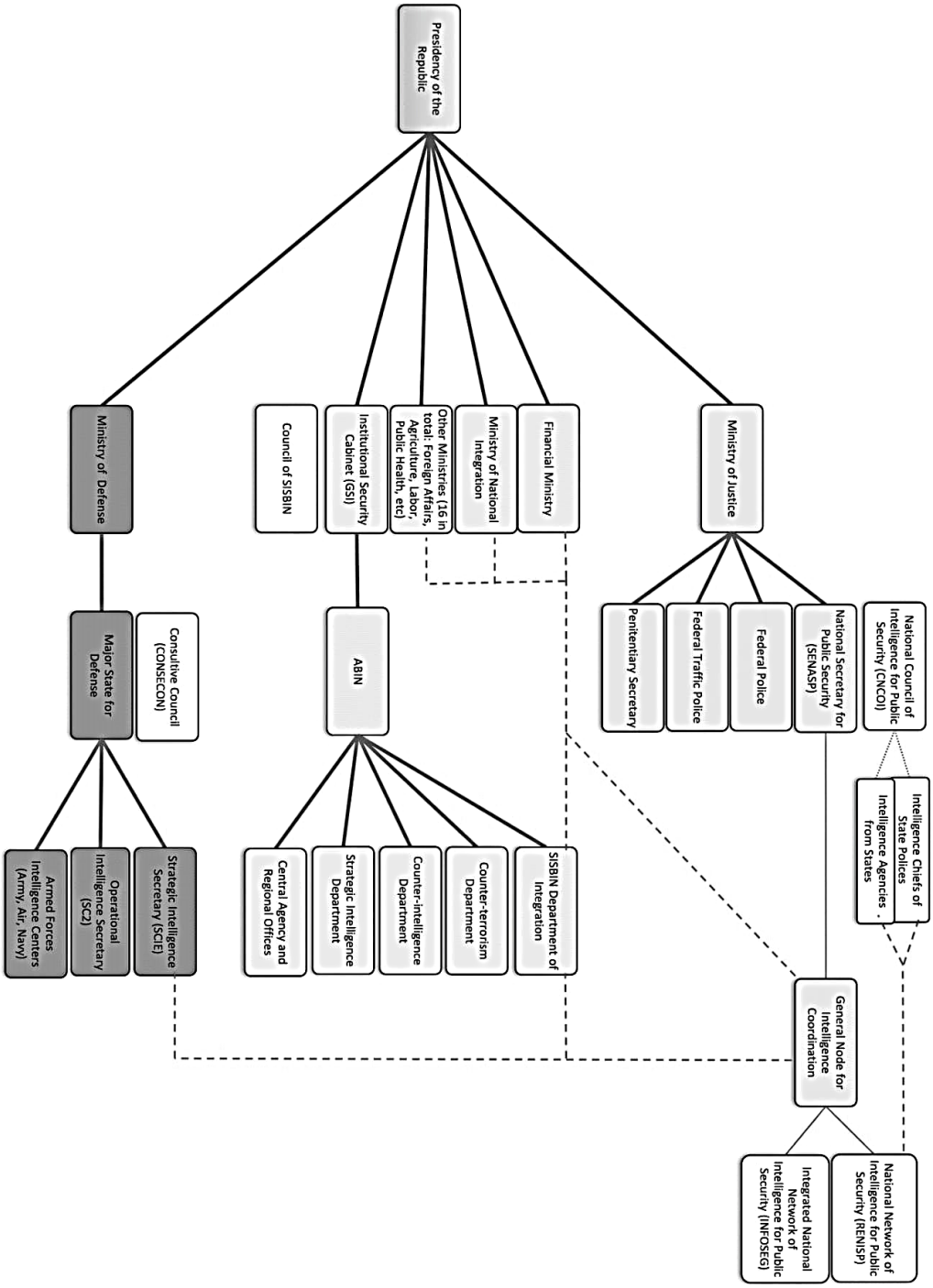
Moreover, the GSI alienated the ABIN in critical moments, such as after the Snowden revelations on surveillance of Brazilian leaders' by the US National Security Agency (NSA) in 2013. The GSI answered to this event with the reallocation of ABIN sections, such as the division of foreign intelligence and the section for technological acquisition, to the Armed Forces. In addition, intelligence analysts complained that the GSI dismantled the ABIN counter-intelligence section (Carpentieri, 2016). In that case, the GSI has shown its capacity to rearticulate the institutional design of the ABIN, assuring the functional supremacy of the intelligence community in Brazil.[42]

In terms of Ethical standards and protocols, Section 2.5 of the National Intelligence Policy (PNI) expresses a set of values and principles. With regard to the behavior of intelligence professionals, the PNI defines that they should preserve "the primacy of truth, keeping honor and personal conduct by clear forms and without subterfuges". In the activity of Intelligence, "ethical values must limit the action of professionals and users… [promoting] unconditional adherence to what society expects from its leaders and servants". However, the PNI does not explain the understating of those values, including those that society requires from intelligence officials. As in the Spanish case, the ethical principles express generic concepts that each agent and analyst should consider in the accomplishment of ABIN and SISBIN missions. That is, in expressing those values, the intelligence community tries to show responsibility for the use of special procedures allowed by law. In that aspect, the PNI (section 2.6) mentions that intelligence activity must be careful to "identify threats, risks and opportunities to the country and the population". Thus, "it is important that individual and collective capacities, available at universities, research centers, and other public and private institutions, collaborate with intelligence", in order to "contributing with the society and the State to pursue their objectives". Yet, again, there no explicit mention to those objectives.

[42] The GSI also acts as a crucial leader of the National Security Council and the Chamber of Foreign Relations and National Defense (CREDEN). The CREDEN was born through Decree No. 4.801/2003 as a sector for internal control and administration for the Executive. Since then, the CREDEN implements actions and programs regarding international security, defense, borders, population, human rights, peace operations, drug trafficking, international crimes, immigration, intelligence activities, critical infrastructures, information security, and cyber security. Officials from several ministries have a place in the CREDEN, but the GSI controls the structure and the functions (Carpentieri, 2016).

As a final remark, it must be said that the development of information and communication technologies are new fronts to the Brazilian intelligence community. Those aspects impose the need for updating means and methods with regard to data processing, storage, and protection of systems. As in the case of the Spanish CNI Cryptologic Center, the ABIN also has expressed the increasing importance to produce and consume information technologies to ensure the security of the state and society. Due to the vulnerability of electronic systems, as attested in the case of the NSA surveillance programs that targeted Brazilian leaders, the protection of infrastructures in the cyber-space is still a challenge for the intelligence community. Meanwhile, the SISBIN also gives attention to another type of problems, such as "financial crime, organized crime, international drug trafficking, violations of human rights, terrorism, and illegal activities involving the trade or exchange of goods and sensitive technologies that challenge democratic states" (section 3, Decree 8.793/2016). These phenomena, which initially could be considered as matters for the Federal Police and enforcement agencies, are also crucial for the strategic intelligence developed by the ABIN-SISBIN. The convergence between strategic intelligence and police intelligence shows that both fields are intertwined nowadays. In addition, the intelligence strategic realm, as in the past, shows its capacity to spread and merge into other arenas insofar as the threats from criminal activities could undermine the very position of the state, as well as its legitimacy before the public. The increasing interdependency between security and intelligence, and the complexity of risks, redefine the environment in which the agencies operate and emphasizes the importance of sharing and coordinating the dissemination of intelligence.

Figure 10: The Brazilian intelligence community and the ABIN (at federal level)



Source: The Author

Epilogue

In the internal control (control of executive bodies) of intelligence agencies in Spain and Brazil, a crucial question is to avoid the cooptation of those services in the hands of governments, in order to separate this strategic realm from conjectural and partisan issues. At the same time, it is of importance to avoid the transformation of those services into total autonomous institutions, resembling parallel organizations outside the control from the Executive. The latter point is of importance as agencies may also autonomously adopt external and internal defense strategies to defend their political guidelines, constituting themselves as parallel governments.

In the internal control, a crucial issue emerges because the intelligence agencies are structurally *sui generis* public agencies, hierarchically linked to the Executive Branch - who periodically elaborate a national intelligence policy - and subjected to a special legal regime that regulates their organization and functioning. In that sense, the internal control of intelligence requires a close yet distant supervision. To simultaneously restrain itself and control intelligence services, states have created diffuse bureaucratic structures with specific attributions and competencies, usually concentrating supervisory roles and coordination in units capable of establishing protocols of joint action, such as the CNI and the ABIN (see previous figures 9 and 10).

In the case of Spain, the CNI legislation passed in May 2002 regulated the main duties and mechanisms for the administration of the Center. By this legislation, the main mission of the CNI is to provide the Government with the information and intelligence necessary to "prevent and avoid any risk or threat that affects the independence and integrity of Spain, the national interests and the stability of institutions and the Rule of law" (Art. 1-3). The Center is attached to the Ministry of Defense and its objectives are defined by the Government, via the Council of Ministers, and reflected in the Intelligence Directive. In addition, the Secretary of State and Director of the National Intelligence Center is appointed on the proposal of the Minister of Defense (art. 9).

Moreover, the internal control of the CNI in terms of funding is regulated by several acts, such as the General Budgetary Law for Public Bodies (amending the tenth additional provision of Law 6/1997), Law 11/95 of March 11 on the use and control of the credits destined to Reserved Funds, and Royal Decree 593/2002. Those rules put the CNI under the financial control of the General Intervention of the State Administration and the Court of Accounts. Finally, the National Intelligence Center is subjected to supervision in terms of its effectiveness by the Ministry of Defense, a kind of control that complements the ones performed by the General Intervention of the State Administration and the Court of Accounts in the

terms of the General Budgetary Law. Finally, added to the financial control, internal ethical protocols regulate the activities within the Center.

In the case of Brazil, the ABIN-SISBIN was enacted by Law 9.883/1999 with the mission to protect "the national sovereignty, the defense of the Democratic State of Law and the dignity of human beings" (Art. 1). The legislation also demands "respect and preserving individual rights and guarantees as well as other provisions from the Federal Constitution […] (Art. 1)". The National Intelligence Policy, established by the President of the Republic since 2009, is developed by the ABIN under supervision of the Chamber of Foreign Relations and National Defense of the Governing Council. In addition, the President of the Republic has authority to nominate the ABIN General Director after consent of the Federal Senate (Art. 11). The ABIN is supervised by the "Consultative Council of the Brazilian Intelligence System" attached to the Secretariat of Government of the Presidency. The Council proposes general norms and procedures for the exchange of knowledge and communications within the SISBIN. In addition, the ABIN is directly subordinated to the Cabinet of Institutional Security (GSI), which shields ABIN from direct contact with the President. The GSI Chief is a high-ranked military appointed by the Executive and the Congress. However, it is still unclear to whom the intelligence system would respond in cases of failure, deviation of power, and alleged inefficiency aside from the ABIN accountability actions to legislative bodies.

Other forms of internal controls are the Management Reports published each year by the Agency. To preserve secret sources, those reports are generic in their description and do not present evaluations of budgets and intelligence programs. Furthermore, "Corregedoria Geral" (COGER), an agency of direct and immediate assistance to the ABIN General Director, investigates infractions and implements disciplinary actions committed by ABIN members. The agency also has *Ouvidorias Gerais*, a sort of Ombudsman or body for internal control. However, *ABIN Ouvidoria* is part of the structure of the Office of the Director-General and lacks operational independence.

Considering both the Spanish and Brazilian cases, the internal controls over the main intelligence agencies depended on the mentioned administrative regulations and accounting rules. Yet, the controls also depended on the supervision and "informal" willingness of masters and policy-makers; as well as in the bargains of power between the Military and Diplomats over the realm of strategic state intelligence. In these battles, one can affirm that internal controls have emerged in order to restrain the military, especially after authoritarian regimes. Likewise the discussion on punitive power and the penal system, the discussion to control intelligence presents itself as the attempt to limit the right to punish, surveille and monitor menaces in times of peace. To leave a logic of unlimited surveillance that ensembles authoritarian regimes, a set of rules and

administrative mechanisms of control have emerged as accountability actions to promote the legality and efficiency of intelligence bureaucracies.

However, in order to be legitimate, the legal and administrative principles should be calibrated in two forms. Firstly, those same principles should establish clear lines to intelligence activities, separating the limits and possibilities of their actions. Secondly, the principles should process the willingness of the people, that is, the accomplishment of mandates stemmed from the sovereignty of the people, in order to be more legitimate.

In the first point, intelligence is a process of governmentality, a power relationship between the exercise of power and the construction of knowledge to manage the security of the state and the sociopolitical order. Intelligence works like a mechanism that, at the same time, deploys forms of domination by watching target groups, and preserves its secret nature to neutralize competitors and create specific knowledge to state-watchers. In that case, it is important to update and define continuously the scopes and legal limits of intelligence, especially if we consider that in the last five decades there were huge technological changes and organizational redefinitions. The current trend in which those agencies work stealthily on an amorphous mass of data (to collect, select, analyze, and create knowledge), reflects the calibration of forces between watchers and watched (especially because the product will be used against a target that might eventually offer some resistance). Thus, implicit relationships of power and technical-scientific forms of governing are at stake, insofar as strategic intelligence has the purpose to construct specific information under the criteria of state security that is part of the surveillant assemblage; a part in the broader mechanisms of surveillance that permeate society. We will readdress the relationship between intelligence and surveillance in Chapter 4.

In the second point, aside from defining the limits of intelligence and forms to produce specific knowledge to the state, the internal controls should enhance legitimate actions. That is, intelligence procedures should be connected, in a certain way, to the sources of legitimacy that hinge on the relations between agents and principals - the people and the representatives of the people who have authority, via elections, to constitute bureaucracies and policies. This is because a ruler or a group might take decisions because they have authority given by the people, but the same decisions might lack legitimacy if they "forget" the sources of legitimacy in a posteriori moment. On the contrary, if those decisions are taken considering citizens, either in terms of representation, participation, transparency, and rule of law, it is said that those decisions have more legitimacy before the public (Koppell, 2010). Those ingredients do not define legitimacy, but the presence of them (even if one is absent) paves the road to a legitimate decision. At the same time, authority is not spontaneous neither is a miraculous practice. Authority takes decisions (normative, cognitive, symbolic, pragmatic) considering

legitimacy either as a procedure or as a consequence. In the former case, the authority to execute a decision is permeable to the steps of legitimacy during the adoption and implementation of a public decision. In a consequential approach, authority considers legitimacy as a result rather than as a means to take and implement a public decision. In both cases, accountability restrains authority to promote legitimacy, either checking or assessing political decisions by their motivations and results. Thus, the point here is to recognize that authority and legitimacy disputes are at stake to decide and implement intelligence policies.

In that sense, table 8 shows how the internal controls, understood as accountability actions upon the CNI and the ABIN, aimed to promote a certain level of legitimacy of intelligence agencies. In the last five decades, we expressed that the agencies started to be more accountable to the Executive in each country. In both cases, they were supposed to be accountable by the strategic intelligence knowledge to protect the state and the socio-political order, which included the stability of the institutions, the national interests, territorial integrity, and the monitoring of key groups and individuals. In order to ensure those goals, it was necessary to deploy several mechanisms to guarantee a certain degree of internal control to tame the agencies. In this perspective, we mentioned the creation of specific legislation and constitutional roles, the National Directives of Intelligence (Spain) and National Policy of Intelligence (Brazil), the extensive administrative law to coordinate the CNI and the SISBIN, as well as auditing ways of supervision and ethical protocols within the agencies.

Table 8: Accountability in the internal control.

Accountability dimensions	Cases	
	Spain	Brazil
Who is accountable?	National Intelligence Agency (CNI)	Brazilian Intelligence Agency (ABIN) as coordinator of the SISBIN
To whom it is accountable?	- To the Executive (especially in the case of CNI)	- To the Executive (especially in the case of ABIN)
About what it is accountable?	Knowledge developed by strategic intelligence to protect the state and the socio-political order, including the stability of institutions, national interests, territorial integrity, and monitoring of key groups and individuals.	Knowledge developed by strategic intelligence to protect the state and the socio-political order, including the stability of institutions, national interests, territorial integrity, and monitoring of key groups and individuals.
How are they accountable? (measures)	Legislation and Constitutional roles. National Directives of Intelligence Auditing supervision Ethical protocols	Legislation and Constitutional roles. National Policy of Intelligence Auditing supervision Ethical protocols

Assessing accountability	Did the accountability action result or promote at least one of the following principles? -Responsibility ~~-Transparency~~ ~~-Answerability~~ ~~-Enforcement (punishment)~~	Did the accountability action result or promote at least one of the following principles? -Responsibility ~~-Transparency~~ ~~-Answerability~~ ~~-Enforcement (punishment)~~

Source: author

According to our methodological operationalization, the performance of public accountability as a connector between authority and sovereignty is a point that must be considered in order to assess its quality. When one authority is called to give an account, if that action does not entail more legitimacy, then accountability fails to reach its objective. In that logic, when an authority from intelligence is called to be accountable by soft means, as in the case of internal controls, it is possible to speak of accountability by responsibility. When intelligence authorities show responsibility (by fulfilling legal duties and mandates), accountability turns up creating new sources of legitimacy by reconsidering the people that authority is supposed to represent. This is the case of administrative forms to turn actors more responsible, in order to synchronize the mentioned relationship between agents and principals. Corruption and deviation of power, for example, undermine the representation of principals, of citizens. By demanding a procedural or administrative account, this simpler form of accountability seeks to re-establish the Schumpeterian notion of political representation of citizens and groups of interest in contemporary democracies. In this procedural and soft approach, accountability seeks to re-create or maintain the socio-political order: the polity and the consolidation of its administrative processes. In other words, by showing responsibility and represent indirectly the voices of citizens after elections and formation of governments, showing responsibility enacts the conditions to perpetuate the intelligence procedures and institutions as well as the sociopolitical order as a whole.

Hence, the administrative and institutional designs to manage and construct intelligence can be considered as primary forms of accountability. That is, they work as self-restraining mechanisms that governments and the administrations used to control the activity of intelligence, giving preeminence either to the CNI or to the ABIN in each country. The institutional designs can be considered as attempts to demonstrate that "something is being done" in terms of intelligence. They are the first step that encompasses and demonstrates the functions, tasks, principles, and rules that guide this activity. The last decades have been a time of enabling internal controls after political transitions from authoritarian regimes. Thus, development and efficiency of internal controls still need to be improved in order to reconsider the mandates and the authority given to those institutions by the people, an authority translated via indirect forms such as the election of governments and coalitions that in turn will establish the directives and missions to intelligence bureaucracies.

Even if internal controls are fully developed (which is still necessary in our cases), this kind of control is a basic and insufficient form of accountability as other principles as transparency, answerability, and enforcement still need to converge and reinforce legitimacy. Thus, now we turn into parallel mechanisms enhanced by alternative forms of accountability. The first of them relates to the role of Legislative bodies.

3.5. Legislative control

Parliaments and Legislative Houses elected by the people can also demand accountability from intelligence services. This implies in control: the supervision, enforcement, inspection, and verification of the government's guidelines for intelligence (Estévez, 2000). Moreover, control also entails overseeing the regulations or administrative orders that guide intelligence (Gill, 2003). In that sense, the first aim of control is to increase the degree of legitimacy of intelligence: The control should ensure that the intelligence activity is performed according to the legal system, the constitutional legislation, and ethical principles. More explicitly, the legislative control assures that intelligence does not violate the set of constitutional guarantees in a country, and when they do so, control bodies as Parliaments are to demand answerability of the motives and outcomes that sustained such violations.

Some scholars also express that the second objective of legislative control is efficiency (Antunes, 2002; Cepik, 2003). In this vision, the control seeks to ensure that the development of the intelligence activity depends on setting appropriate objectives and norms to intelligence. This kind of accountability associates the means available to the intelligence agencies to the performance of their tasks, regarding reserved funds, the exclusive prerogatives to secure the state, and the degree of confidentiality required. Duplication of functions is an example of squandering funds in this activity. Thus, it is necessary to set clear rules and professionalize this activity to avoid efficiency deficits.

Naturally, legitimacy and efficiency are interconnected and should be the main criteria to establish controls over this area. Yet, according to our theoretical and methodological plan, this study is more related to the first kind of control (legitimacy) as we assume that the main goal of an accountable action is to establish a dialectical relation between authority and legitimacy. It does not exclude that efficiency is crucial to the equation. Efficiency is as important as legitimacy for intelligence agencies. Yet, the question of legitimacy has been less addressed in the literature, and we believe that many intelligence agencies demand efficiency (more resources, more cooperation, more professionalization, in short,

more security) as a patch to cover its legitimacy deficits. If an intelligence institution wants to be more legitimate to the eyes of its masters and the public, it should consider the citizens beyond the role of passive figures and submit itself to accountable actions beyond the primary necessities of improving its internal efficiency, i.e. resources, operations, tactics, and strategies.

To be more legitimate, Saín (1999) argues that the parliamentary control should include the inspection of all operations and tasks performed by intelligence agencies, the set of sources and procedures for obtaining data and information, the identity of the agents in charge of operations, and the reasons that justify the conditions of secrecy. This control should also relate to the existing files, the reports produced, the set of confidential norms, as well as all the expenses destined to intelligence. The regular and simultaneous development of those controls would allow controlling the legitimacy of intelligence activities, as well as the quality of the efficiency of intelligence professionals.

In that sense, this section explores whether the main accountability actions implemented by the Parliament in Spain and Brazil enabled the control of intelligence especially in terms of legitimacy but also of efficiency. Firstly, we will expose the legal designs and norms that define the Parliament's role when it comes to scrutinizing intelligence agencies, as well as the dilemmas in this kind of control. Secondly, we will discuss the main episodes and events regarding the Legislative control in both countries. Finally, we will analyze the role of Parliaments as demanders of accountability and the results of these controls.

In Spain, when the CESID was created in 1977, the legislative or parliamentary control of the information/intelligence activity was barely recognized. As we mentioned, the CESID professionalization and expansion occurred especially after the *Fenix Plan* in the 1980s. After this phase, the increasing role of the Spanish Parliament in the political life of the country lead to promote the control of intelligence activities. In the early 1990s, a series of power deviation put the Center in the political agenda of the country. Cases of irregular use of reserved funds (cases Rubio, Roldán, and Banesto) involved the CESID and demanded attention by different parliamentary members, enacting the first commission of control for intelligence in 1995. In this year, the Parliament established an Act to demand regular accounts from the Executive regarding the use of reserved funds. However, the government did not comply with the obligation of delivering and presenting reports. The effective institutionalization of Parliament secret commissions was only achieved after the reform of the CNI in 2002 (Ruiz Miguel, 2005).

When the mentioned corruption scandals emerged, the events revealed a paradox. Parliament members demanded more mechanisms to access official secrets of the state. However, they faced difficulties to disclose incomes and

budgets because the Executive used to manage the reserved funds under heavy secrecy. The so-called "Commission of Official Secrets" established during the 1990s was famous and its members reached certain publicity after the media coverage on espionage services. Yet, according to the Presidency of the Congress, "there were no official procedures to regulate the access to official secrets" (Bueso, 1997, p. 29). In practice, all the parliamentary activities lacked formalization. Until the Commission of 1995, "only a few deputies, representing all the Parliamentary Groups, were elected by the Plenary of the House by a majority of three-fifths of the members to meet a member of the Government and the CESID Director". Besides, "the Congress did not specify the authority or the persons who were responsible to disclose official information" (Bueso, 1997, p. 30).

Moreover, Congressmen did not know if they were obliged to reveal secret information to the judicial power in case of obtaining proof of wrongdoing and corruption. Representatives knew that every citizen has the constitutional obligation to collaborate with Justice when required by judges and courts in the instruction of a process (Article 118 Spanish Constitution). To avoid clashes against the Executive, the act of 1995 demanded Congressmen to keep secrecy about classified information and documents accessed in their role of controllers of the government. Disobeying these terms allowed penal instructions over the members of the Parliament. Thus, despite the capacity to create Investigative Parliamentary Commissions to control the activity of intelligence, the representatives were forbidden to use this kind of control as proof or evidence to support Justice.

In that sense, Law 11/1995, of May 11, was the milestone to regulate the use and control of credits destined to reserved expenditures. According to it, reserved credits or funds are those expenses incorporated in the General State Budget to cover expenses deemed as necessary for the defense and security of the State (art. 1). Those expenses are not public and have a special system of justification and control. The credits destined to reserved expenditures are proposed every fiscal year in the General State Budget Law (art. 2) and any budgetary modification in relation to such credits shall be authorized by the Parliament. Moreover, all the information related to those credits is classified in compliance with the Law of Official Secrets (art. 3). In addition, the credits are only used to support certain institutions: the Ministries of Foreign Affairs, Defense, Interior, and the intelligence services (art. 4). The Ministries and Departments determine the purpose and destination of the funds and the authorities to manage their use. The discretional power to allocate State budgets and apply reserved credits was narrowed especially after the fiscal austerity measures that were enhanced by the Spanish Administration since 2008, such as Royal Decree 20/2011 to reduce the public financial debt.

It is important to know that Law 11/1995 also enhances legislative control over the reserved credits, establishing rules for the organization of the Parliamentary Commission. "The appropriation and destination of reserved credits will be subjected to the control of the Congress of Deputies, through a Parliamentary Commission composed by the President of the Chamber and those Congressmen who have access to official secrets in accordance with parliamentary regulations" (art. 7). Moreover, the Ministries and managers of the departments that receive reserved credits shall report to the Commission every six months in order to inform the application and use of these funds. To do so, the sessions of the Commission are held in secret and the members are obligated to preserve confidentiality.

As observed, Law 11/1995 tried to solve the previous tensions that could emerge in the control of a sensitive realm. However, it does mean that the tensions are over. In a legal interpretation, the Executive can oppose the request of the Congress appealing to the self-limitation power of the Legislative branch or to the legal necessity to impose secrecy.[43] Besides, not to disclosing information might be justified on limitations expressed by the Constitution, such as safeguarding the right to honor, to personal and family privacy, as well as to individual image (Article 18.1). In that logic, it is important to remind the array of rights that are protected and should not be published, such as secrecy of communications (postal, telegraphic, telephonic, etc.) (Article 18.3); labor or professional secrecy (article 20.1º, d), and the prohibition for citizens to access the archives and records that affect the security and defense of the state, the investigation of crimes, and the privacy of persons (article 105, b).

On the contrary, the right of the Parliament to request information is enacted by two mechanisms. First, to accomplish demands of the Parliamentary Commission under the provisions of Articles 109, 110, and 111 of the Constitution. Second, to guarantee legislators their rights as representatives of the people guaranteed by article 23.2 of the Constitution. Hence, it is only possible for the Government to deny the request for information from a parliamentary body or representative based on the obligation to defend constitutional rights. Nevertheless, the Government or the requested Administration will not be able to deny the requested documentation if it is possible to conciliate, in reasonable terms, the right of the Congressmen to the documentation with the protection of constitutional rights that hypothetically could result affected. The problem, then, is to balance judicially and politically the clashing parts in every situation. As specific documentation is necessary for the deputy to exercise his/her functions, the denial of the documents, in absolute terms, is only reasonable if protected by powerful juridical-constitutional motivations. The exemption or limitation of the

[43] For example, Law 9/1968 modified by Law 48/1978 of Official Secrets, Article 10.2 states that this law will not affect the Congress or the Senate, but its application has generated the mentioned accountability dilemmas.

Administration to the parliamentary control supposes a "sacrifice of the principles that govern a constitutional system and could lead to an enormous judicial clash" (Bueso, 1997, p. 22). Therefore, the means to provide the Parliament or the Congress Commission with the required documentation should be explicit as in the case of Law 11/1995.

Besides judicial and constitutional matters, functionality principles also affect the role of Parliament to oversee the Executive. Law 11/1995, regarding the Parliament control of reserved credits, only certain parliamentary groups, representing at least one-quarter of the House, can request information on classified matters and always through the Presidency of the Parliament. This is a first limit that expresses that only the powerful Parliamentary Groups, understood as main actors in the life of the Chamber, would exercise accountability roles. For those groups with underrepresentation, there is a lack of discretional ability to request accountable actions from the Executive, even when political parties have a solid constitutional and regulatory base as "fundamental instruments for political participation" (Art. 6, Spanish Constitution, 1977).

Another functional principle is that the Executive discloses information based on the level of its classification. If the classification corresponded to the category of "secret", the Government provides the information to a member of each Parliamentary Group in accordance with the provisions of Article 23.1 of Law 11/1995. By this, those members should be elected for that purpose by the Plenary of a three-fifths majority. After the creation of the CNI, Resolution of the Presidency of the Congress of Deputies, of May 11, 2004, also regulated the functioning work of the Commission to control the reserved credits and, by extension, intelligence. According to the new Resolution, "the Commissions and one or more Parliamentary Groups that include at least a quarter of the members of the Congress may request, through the Presidency of the Chamber, to be informed about matters that have been declared classified according to the Law on Official Secrets" (Art. 1). It also defines that the Executive might provide secret information to one representative of each Parliamentary Group. The House, by a majority of three fifths in the plenary sessions, elects the representatives for those cases (art. 3).

On the other hand, according to Resolution of May 11, 2004, the Executive will provide information classified in the category of "reserved" to the Spokesmen of the Parliamentary Groups or to the representatives in the Commission (art. 4). In exceptional cases, the Executive might request to provide the information on a certain matter declared as secret only to the President of the Congress or to the President of the Commission. Furthermore, the Executive might request to provide reserved information in secret sessions. In these cases, only members of the Commission may attend the information session (art. 6). When the information collected refers to the content of a document, the accountable authority will

provide the representative the original version or a copy of the documentation. Representatives are able to request more information in case they consider the documentation is incomplete or to demand specific knowledge about the classified matter (art. 7). In addition, Representatives chosen to this kind of control might examine the documentation, in the presence of the authority that provides it, and take notes, but they never can obtain copies of those materials. The documents are examined in the Congress or in the location they are stored, but only after the approval of the President of the Congress (art. 8).

The rules expressed above define the role of the Parliament in terms of access to secret and reserved matters and to the control of reserved credits. However, the rules were not easily formulated. At the time of the creation of the CNI in 2002, the Parliament proposed two projects in the Defense Commission to define the normative text to establish the external accountability of the Center. On February 20, 2002, the Commission discussed the CNI's Regulatory Law Proposal that we commented in the previous section (Law 11/2002). Later on, the Commission debated the Organic Regulatory Law Proposal related to Previous Judicial Control of the National Intelligence Center. On March 7, the mandatory deliberation process was held in the House, and after the approval, the text was sent to the Senate. There, senators formulated four veto actions to the proposals: three by the Mixed Group, and one by the Basque Nationalist Group. Those groups considered the law proposals as a threat to the rights and freedoms of citizens. According to them, the Government prioritized security over freedom after the 9/11 attacks in New York in 2001. They criticized that the intelligence aimed to obtain a legal shield or mask to operate security above parliamentary and judicial rights. In their vision, the projects did not solve the deficient parliamentary control of the activity of the CNI and the practical absence of real judicial control in the prior authorization of the Spanish secret services. In addition, the Project ignored that the "Spanish State is autonomous and the coordination between the state intelligence services and the intelligence linked to the police of the Autonomous Communities was not foreseen" (Aba-Catoira, 2002, pág. 150). The Senate rejected the four veto proposals and the eighty-one amend proposals presented in the House. On April 18, after intense deliberation, the Senate agreed to accept the text as submitted by the Congress of Deputies. Finally, in the session of April 24, the Senators approved the projects without modifications.

The projects were published in the Law of May 06, 2002, as commented in the previous section of internal control. As indicated, the Law enshrined the legal configuration of the National Intelligence Center (CNI) in Spain. According to Chapter III, the CNI is submitted to Parliamentary control in the following terms:

> 1. The National Intelligence Center shall submit to the Congress of Deputies, in the forms provided by its Regulation, and through the Commission for the control of reserved credits chaired by the President of the Chamber, the appropriate information of intelligence operations

> and activities. The content of the sessions and the deliberation will be secret.
>
> 2. The aforementioned Commission of the Congress of Deputies will access the classified matters, with the exception of those related to the sources and means of the National Intelligence Center and those that derive from foreign services or international organizations in the terms established in the corresponding agreements for the exchange of classified information.
>
> 3. The members of the Commission are obligated, in the terms of the Regulations of the Congress of Deputies, to keep secrecy about the information and documents they receive. Once the member analyze the documents, these will return to the National Intelligence Center for proper custody, without option to retain original versions or copies.
>
> 4. The Commission referred in this article will be informed of the intelligence objectives established annually by the Government. The reports will be prepared by the Director of the National Intelligence Center to evaluate the activities, the status, and the degree of compliance with the objectives indicated for the term (Art. 11, Law 11/2002).

As attested by paragraph 1, the Parliament Commission that oversees the CNI activities is the same Parliamentary body created to control the mentioned Reserved Credits for national security purposes. Despite the right to oversee the intelligence agency, Paragraph 2 expresses that Congressmen would not be able to control procedures and documents that the Executive consider as sensitives to National Security purposes as well as those parts that compromise liaisons and links with foreign intelligence services – for example, the intelligence cooperation shared with the NATO members and other allied nations. This is an important point that will be addressed in the international mechanisms of accountability (see Section 3.7 of this Chapter). Law 11/2002 also mentions that Congressmen are obligated to keep secrecy and not reveal classified information that they could receive. Again, the Center has the *potestas* to release and reveal what it considers appropriate to the Parliament. Since Congressmen usually do not know internal procedures and protocols of intelligence, the control over the CNI depends on the very predisposition of this agency to be controlled. This reminds the "situation 3" in terms of asymmetry of power related to the efficiency of accountability, as analyzed in the theoretical part (Chapter 1). A situation in which the accountant dictates the agenda and the topics of the accounting action. In that sense, the Parliament assesses the CNI according to the plans and objectives settled by the Executive. Law 11/2002, in addition, established a minimum frequency to the legislative control, as the Director of the CNI needs to show the objectives assigned to the Center at least once a year.

The basic legislative control enshrined by Law 11/2002 tries to solve old dilemmas in the clash between the Executive and the Legislative regarding the classification and disclosing of state secrets. That clash is produced because state

secrets are regulated and are a competence of the Council of Ministers. Aside from the internal or Executive control, there is a lack of control to verify the justification and the procedures that motivate the classification of any information by the Council. Moreover, another obstacle to accountability is that the Council of Ministers was traditionally the only body with competence to classify or declassify state secrets, holding this monopoly on national security and defense grounds. Thus, it was necessary at least some reforms to alter the State and Official Secrets Law of 1977. The first of those reforms allowed the Congress and the Senate to access classified matters in 1986 (Aba-Catoira, 2002), followed by Resolution of the Presidency of the Congress of June 2, 1992, and by the aforementioned Law 11 of 1995, which allowed the Parliament to exercise more controls to the Executive. In that sense, Law 11/2002 that regulates the CNI tries to complement and reassure the content dictated by Law 11/1995. Instead of a reformulation of the Parliamentary role to control intelligence, it could be said that the latter rule just updated the previous ones. Despite those reforms, scholars like Revenga (2001) (2003) affirm that the parliamentary control of the CNI and other intelligence agencies is defective because the Executive itself answers politically for the management of the intelligence activity before the Parliament. For him, there are no specific administrative outcomes in case the CNI fails to give accounts to the Parliament. Meanwhile, the accounts of the CNI Directors would resemble general promises of improvement and vague political statements to appease the legislators. To verify and assess if those deficits are true, now we address the mains events and history of the legislative control of intelligence in Spain.

The Parliament Commission for the Control de Reserved Credits existed since the CESID years. However, this control was only regulated in 1992 and 1995 and obtained a constitutional status by Law 11/2002. Literature about the activities of this commission during the CESID is scarce. For example, Díaz-Fernández (2005) wrote a crucial study on the Parliament initiatives and controls deployed over the CESID from legislatures I to VII in Spain. His study covers the history of the Commissions from 1977 to 2002. He divided the Parliament control into the following domains: Economy, structure (of intelligence), functions, international, judicial, personnel or staff, and other (miscellanea). The criteria for that division is not clear, yet, he offers a valuable panorama about the characteristics and topics used by Parliament representatives to hold accountable the intelligence services. As many of the accountability actions are initiated by different authors, the table below depicts the number of initiatives according to the parliamentary groups and the Government (when it gives accounts obligated by law or by its initiative).

Table 9: Parliament initiatives to control the SECID activities (1977-2002)

Parliament Group	Content of the Parliament Initiatives						
	Economy	Structure	Functions	International	Judicial	Personnel	Other
Socialist	-	-	7	1	1	1	4
Popular	7	9	24	4	2	5	10
Catalan	1	-	1	-	-	-	-
Canarias	1	-	2	-	-	-	-
IU	19	11	34	8	10	16	21
Basque	-	-	2	-	-	-	4
Government	-	1	4	-	-	1	1
CDS	-	4	-	-	-	-	-
Mixed Group	-	-	14	4	8	3	6
Total	28	25	88	17	21	26	47
Total (%)	11.1	9.9	34.9	6.7	8.3	10.3	18.6

Source: (Díaz-Fernández, 2005, p. 311).

As the table shows, most of the Parliament commissions were motivated to control intelligence functions (34.9% of initiatives). This expresses that representatives had a certain lack of knowledge to understand intelligence missions and tasks. For example, they wanted to know the objects of intelligence, the main operations, and the objectives in this realm. The accountable actions related to institutional designs and organizational structure were not addressed, for instance, in the same intensity as personnel (professionalization of intelligence) (10.3% of the initiatives), economy (budget and reserved credits use) (11.1% of the initiatives), international (relations with foreign intelligence services and counter-intelligence) (6.7%), and other issues (18.6%).

The number of initiatives does not show whether the CESID was effectively controlled or not. Despite this, the table offers an idea regarding the type and volume of activities from the parliament. It is important to notice that opposition parties have conducted many of the initiatives in this period. The cases were led by the second-largest opposition group in the years the Socialists government (the Popular group with 61 initiatives), and by the group of Izquierda Unida (98 initiatives), a leftist minority party that found a voice to scrutinize the government. This might be explained because the CESID focused on monitoring groups of this side of the political spectrum acting without external controls at the beginning of the transition. Nonetheless, Díaz-Fernández criticizes the fact that many of those parties, including the nationalists, used this kind of control in a more symbolic than effective way. To him, many initiatives from nationalists consisted of asking generic questions or accusing through inquisitive methods, that is, based on rumors to obtain information that would support their narratives. The nationalist groups, however, have not acted homogeneously or based solely on their interests, since most of their initiatives appear sporadically or are scarce as seen in the table (2 initiatives by the Catalan, 3 by Canarias, and 6 by the Basques).

On the other hand, Díaz-Fernández mentions that the Executive has systematically used three formulas over the twenty-five years analyzed in the table. The first was to respond in a simple and summarized way to the requirements of the deputies, even showing a lack of interest to respond to the parliament initiatives. Secondly, the Government answered denying facts or information about the CESID. In those cases, the Government mentioned that the legal norms did not allow intelligence to carry out certain types of operations. For example, intelligence officials say that they do not develop monitoring actions or espionage because Law does not allow intelligence services to do so. Thirdly, another way to shield the agency was appealing to secrecy norms to avoid the disclosure of information. However, it is hard to prove that these techniques were systematically used by the service.

After the CNI creation in 2002, the literature related to the Legislative control is even scarcer. Thus, we have consulted the main database of the Congress of Deputies to elaborate a different analysis of the Legislative control during the last decades. Instead of creating a table as in the case of the CESID years, we think that the last years deserve a detailed approach regarding the work of the Commission for Reserved Credits. This effort comes to complement the work of researchers like Díaz-Fernández in his analysis of the Legislative control in a previous period (from Legislature I until Legislature VII). Thus, we will address the work promoted by the Spanish Parliament in each legislature from 2004 to 2019 (From Legislature VIII to Legislature XII). To do this, specific content of each session is not available since they are covered by secrecy or are reserved to members of the commission. Thus, the available information relates to a search conducted in the Congress of Deputies database. The search return entries according to the date of the Commissions, the motive of the initiative, the Parliament group who initiated or requested the accountable action, and the result of the initiative (processed without accordance, rejected or expired) (See Annex I in Appendices).

During the Legislature VIII (2004-2008), the Commission for Reserved Credits conducted 29 initiatives. The complete list of those initiatives can be consulted in Annex I. Here we will comment the most important ones regarding the legitimacy and efficiency of the CNI. During this legislature, almost all the initiatives are related to the Spanish collaboration with the CIA rendition flights, in which the American agency captured alleged terrorists in the Middle East using European airports to transfer them to the USA. In the detention and transportation of prisoners, several denounces of torture and infringement of international human rights treaties were made by society organizations such as International Amnesty and even from the European Parliament who established an Investigative Commission in countries like Germany and Great Britain (Born, Leigh, & Wills, 2011). In the case of Spain, Catalan and Canarias parliamentary groups were the main authors of the initiatives. Yet, most of these proposals were rejected by the

Commission or expired before response of the Government. Those groups demanded the participation of the CNI director, the Ministry of Interior, and the Ministry of Defense to justify the use of Mallorca and Canarias airports by the CIA without consent of the Spanish Justice. After two years of pressure, the Government convoked the Parliament Commission to explain those episodes in June 2006. There is no record of the results about this meeting but it seems that the outcomes were not satisfactory since the Parliament groups continued to formulate initiatives about the CIA flights in the Spanish territory during the next months. More initiatives were promoted due to the secret agreements between the Government and ETA to reach a truce in the terrorist activities of the Basque separatists. Finally, the Popular group demanded explanations of the CNI director about the alleged surveillance of the Center over key business groups, but the initiatives expired. The only successful initiative by the Popular group (the major opposition group at that time) was related to the prosecution of Roberto Flores Garcia, a CNI agent who allegedly disclosed secret files from the Center to Russian liaisons.

During the Legislature IX (2008-2011), the Commission for Reserved Credits conducted 22 initiatives. During the first years of the legislature, Catalan groups continued to formulate initiatives to demand deeper explanations about the CIA rendition flights in Spain. In this period, the Popular group (opposition party) increased the number of initiatives to 5. The first initiative called the Vice-president of the Government to explain the CNI tracking and surveillance over the magistrate Roberto Garcia Calvo (a judge sponsored by the Popular group), but the petition was rejected. The following Popular initiatives demanded official explanations about the removal of the counter-terrorism chief of intelligence; the alleged Russian interference in the company Repsol; the Alakrana ship liberation and the negotiations with Somali pirates; and the nearly 30 substitutions promoted in the CNI office of anti-terrorism during those years. It seems that this division experienced an internal crisis or was targeted by political nominations of the CNI Director and the Executive. For example, the Popular group used this situation to formulate another initiative and convoked the CNI Director to explain the management and internal changes of antiterrorism policies. On the other hand, different groups promoted initiatives to clarify the CNI collaboration with Spanish troops in Afghanistan (Izquierda Unida and Esquerra Republicana groups) and to obtain explanations from the CNI Director about the alleged surveillance of PNV leaders (Basque Nationalist Party) including the Lehendakari Ibarretxe (Basque Prime-Minister). A final category could be related to the formal initiatives promoted by the own Government to communicate the use of Reserved Credits and explain the Directive of Intelligence (the intelligence national plan) each year. This category stems from the legal obligations of the CNI to give accounts before the Parliament Commission, as established by Law 11/2002.

During the Legislature X (2011-2016), the Commission for Reserved Credits conducted 16 initiatives. In this period, the Popular group assumed the Government and the Socialists became opposition, whereas, at the final years of the Legislature, the emergence of new political parties (Podemos, Ciudadanos) lead to a reformulation of the Parliamentary groups (such as the colligation Izquierda Unida-Podemos in the left side of the political spectrum). There is no intention in commenting all the initiatives. However, it is worthy to mention that the Government continued to communicate the use of Reserved Credits and the Directive of Intelligence at least once a year, as established by the Spanish legislation. In parallel, this period appears as the most fragmented in terms of plurality of initiatives and Parliamentary groups. For example, Convergencia i Unió group demanded answers from the CNI about political espionage targeting social and business leaders in Catalonia. The Izquierda Unida colligation group demanded justifications about the use of intelligence funds in the Corinna case (a mistress of the Spanish King that would have been cooptated by the intelligence service to avoid leaks and preserve the Royal House reputation). Besides, the same group was the first to promote an initiative about the counter-intelligence measures taken by Spain in the face of the Snowden revelations and mass surveillance by the NSA (National Security Agency of the USA) in 2013. As the revelations were too serious and redefined the intelligence political agenda across the world, the Spanish Government itself convoked the CNI Director to clarify the NSA surveillance on October 30th. There are no records of the meeting aside of the media coverage after the sessions, in which the Government was relieved by the explanations given by the CNI Director Felix Saenz, who assured that the CNI did not collaborate with the NSA and the Spanish service did not target Spanish citizens and politicians.[44] However, documents revealed by Snowden do not mention the CNI but they prove that the Spanish intelligence collaborated with the NSA to intercept metadata and electronic signals.[45] On November 5th, a final initiative promoted by Izquierda Unida was prepared to demand clarifications of the Snowden Case and the Spanish role in the mass surveillance scandal but this initiative expired. During those years, Basque Nationalists also convoked the CNI director about the alleged espionage of political organizations in the Basque Country as well as in other regions in Spain, but the initiative also expired.

During the Legislature XI (January 2016 – May 2016), due to the extinction of the bipartisan system and the emergence of new groups, the Popular party was

[44] *RTVE*. 2013, November 06th. 'Félix Sanz dice que el CNI no va de "caza" ni espía a políticos y que las escuchas son legales'. Retrieved from: https://www.rtve.es/noticias/20131106/felix-sanz-dice-cni-no-va-caza-ni-espia-politicos-escuchas-son-legales/784781.shtml in 09/17/2019.

[45] Aranda, G. 2013, October 30. 'El CNI facilitó el espionaje masivo de EEUU a España'. *El Mundo*. Retrieved from https://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html in 09/17/2019.

not able to establish a new Government, and no Parliamentary commissions were held for the intelligence activity.

During the Legislature XII (2016 - 2019), the Popular party formed an unstable new Government. In this context, and due to the new colligations and parties, Mariano Rajoy (President of the Government) had the power revoked by other formations, and the Socialists returned to the Executive in 2018. In this period, the Commission for Reserved Credits conducted 19 initiatives. The leftist Unidos-Podemos group promoted the first one to demand answers of the CNI director about the alleged espionage of Podemos Leader, Pablo Iglesias, during his campaign and due to his opposition to the major political formations. The same Parliamentary group promoted initiatives regarding the political espionage of high authorities of the state in 2017, and due to the mentioned Corinna case in 2018. Yet, those initiatives expired or were not accepted. Nationalist group initiatives were related to alleged misuse of Reserved Credits (PNV in 2017 and Esquerra Republicana in 2018). Meanwhile, the Socialists and Ciudadanos groups convoked the CNI director to give explanations about the impact of the WannaCry cyberattack in Spain and the consequences to companies and business organizations in 2018. The socialist group also demanded justifications related to the alleged Russian interference in the Catalonian separatist referendum the same year. In parallel, corruption scandals such as the Villarejo and Bárcenas cases, for bribery and corruption in high spheres of the Ministry of Interior and of the Executive, respectively, resulted in the initiatives of the Mixed group to demand answerability and deeper information related to those episodes in 2018. Finally, when the Popular group became opposition, one initiative was promoted in 2019 to clarify the use of Reserved Credits in international trips of the Socialist President, Pedro Sánchez, during his diplomatic agenda to several countries.

During the Legislature XIII (May 2019 – December 2019), the Socialist Pedro Sánchez did not receive support from other parties for his nomination as President and was not able to establish a new Government, so no Parliamentary commissions were held for the intelligence activity.

During the Legislature XIV (December 2019 -), Pedro Sánchez formed government through a collision with 'Unidas Podemos'. The Commission for Reserved Funds did not hold meetings during this period as a consequence of the pandemic crisis and partisan clashes. The Popular Party opposed to giving access to official secrets to nationalist parties such as EH Bildu (Basque) and Republican Left of Catalonia (ERC). The same veto to ERC was exercised by the Popular Party from 2011 and 2015 as the Catalan party was part of the mixed Parliament group. However, in this legislature both nationalist parties have more representation in the Parliament compared to previous years and the work of the Commission has reached a political impasse. The tensions have also increased since right parties such as VOX were reluctant to integrate 'Unidas Podemos' leftist leaders in the

Commission. Moreover, Catalonian politicians linked with the ERC, such as Roger Torrent and Ernest Maragall, had their phones hacked by espionage software used by governments and security agencies in 2020. The CNI was accused of those interventions but the linkage is hard to be demonstrated. The political tensions have also blocked the work of the Commission to assess the annual Directive of Intelligence established by the Government as well as to check the legality, scope, and range of the CNI activities.[46]

To summarize this section, it can be expressed that the Spanish development of the legislative control has been inconsistent and ineffective most of the time. During the CESID years, the lack of legal norms produced a gap that was not filled as representatives had their access to classified information denied. From 1977 to 1986, the Parliament lacked instruments to access secret information. The regulatory Laws of 1995 and 2004 enacted and reinforced the control, but it has been oriented to review illegal past actions, rather than enabling continuous supervision conducted in a proactive base. As the exhibition of the history of the Parliament initiatives show, the legislative control is remarkably reactive and depending on the agenda and predisposition of the Executive to be efficient. More recently, the performance of the Commission has been blocked due to partisan clashes, alleged fear to disclose information, and reluctance to establish a continuous evaluation of intelligence, especially before nationalist parties that have been potential targets or could have a dubious role to oversee this field. New parties are to reshape their behavior to access secret services beyond their partisan interests. At the same time, an activity related to the core functions of the state should not be outside the range of the representatives of the people, even if new groups have distinct political preferences and visions regarding the establishment. If those tensions increase, intelligence would be amidst a legitimacy crisis that eventually could lead to the crack of the institutional order.

*

As in the case of Spain, now we examine the main legislation regarding the Legislative control of the Brazilian Intelligence System (SISBIN) and the Brazilian Intelligence Agency (ABIN). After this examination, we will address the main episodes and show examples of this control during the last decades.

As mentioned in the section of internal control, Law 9.883 of December 7, 1999, defines the National Congress as the only enhancer of the external control of the intelligence activity. Article 6 mentions that members of the majority and minority groups from the House of Deputies and the Federal Senate exercise the sessions of control. The article also determines that the presidents of the

[46] Rincón, R.; Díez, A. 2020, July 17, 'El bloqueo político impide al Congreso fiscalizar el CNI', *El País* España. Retrived from https://elpais.com/espana/2020-07-16/el-bloqueo-politico-impide-al-congreso-fiscalizar-el-cni.html in 07/17/2020.

Commissions of Foreign Relations and National Defense of the House of Deputies and the Federal Senate are members of the external control body of the intelligence activity. Thus, whereas in Spain only members of the House of Deputies comprise the Commission of Control of Reserved Credits, in Brazil, both legislative houses exercise the external control of intelligence.

Article 6 also defines the Parliamentary group to oversee the execution of the National Intelligence Policy. However, the legislation emphasizes that the ABIN information or documents might only be accessed through the Chief of the Institutional Security Cabinet (GSI) (Art. 7). In other words, the GSI Chief is the only figure who is responsible to supply information to the Parliamentary groups and authorize the official communication of intelligence organizations under his/her command.[47] To avoid leaks or misinformation, the text expresses that any authority or other person who has access to enclosed documents or information is obligated to maintain secrecy to avoid administrative, civil, and criminal sanctions.

When the ABIN-SISBIN was created in 1999, the above articles were the only lines to the Legislative control of intelligence. They defined the basic norms and obligations from intelligence towards the representatives of the Houses. This control is conducted respecting the secrecy and confidentiality of this activity. Yet, the lack of deeper rules and procedures created a vacuum that was not filled until the promulgation of the Resolution N.2 of the Brazilian Congress in 2013, which enacted the Mixed Commission for the Control of Intelligence Activities (CCAI). This Commission was demanded by Article 6 of Law 9.883/1999. In other words, the country lacked a specific regulation to define the work and procedures of the Commission for fourteen years in recent history. This gap caused several problems in terms of efficiency and institutionalization of the Brazilian legislative control, as we will see in the examples ahead.

Resolution n.2 of 2013 of the Brazilian Congress established the Joint Commission for the Control of Intelligence Activities (CCAI) as a permanent committee of the National Congress to exercise the external oversight of the intelligence activity (Art. 1) in accordance with Law 9,883, of 1999. To be precise, the CCAI oversees the intelligence and counterintelligence activities developed in Brazil or abroad by organs and entities of the Federal Public Administration, especially by the ABIN-SISBIN (art. 2). This kind of control should ensure that "such activities are conducted in accordance with the Federal Constitution and with the norms of the national legal system, in defense of individual rights and guarantees of the state and society" (art. 2). According to the Resolution:

[47] According to article 10, Law 9.883/1999: "the ABIN may only communicate with the other bodies of the direct, indirect or foundational public administration of any of the Powers of the Union, of the States, of the Federal District and of the Municipalities, with the prior approval from the competent authority of higher hierarchy attached the mentioned organization."

> Paragraph 1 - For the purposes of this Resolution, oversight and control are understood as all actions related to the supervision, verification and inspection of the activities of persons, organs and entities related to intelligence and counterintelligence, as well as to safeguarding confidential information, aiming the defense of the Rule of law and the protection of the state and society.
>
> Paragraph 2. The control of the intelligence activity conducted by the National Congress comprises the activities carried out by the SISBIN organs throughout the intelligence cycle, such as gathering, gathering or searching, information analysis, knowledge production, and dissemination, as well as the counterintelligence function and any related operations.
>
> Paragraph 3. The attributions of the CCAI comprise, in a non-exclusive way, the inspection and control:
>
> I – of the activities of intelligence and counterintelligence and the safeguard of classified information by organs and entities of the Federal Public Administration in Brazil and the SISBIN, both in Brazil and abroad;
>
> II - of the procedures adopted and results obtained by the organs and entities mentioned in item I;
>
> III - intelligence and counterintelligence actions related to the protection of citizens and democratic institutions;
>
> IV - any intelligence operations carried out by the SISBIN organizations.

As we can see, the control established by the norm is broad and covers the classical understanding of intelligence as a policy cycle. Intelligence here is understood as a process, from the collection to the dissemination of information for decision-making in national security and the safeguard of the country and population. In the same logic, counter-intelligence is understood as the attempt to undermine national intelligence activities as well as those actions that affect the security of the institutions, the state, and society.[48] Moreover, the norm also allows overseeing resources, procedures, and personnel that develop intelligence tasks in the colossal SISBIN system as well as in any Federal Public Administration. Yet, it is not clear how this control should be implemented in the latter case: over the

[48] For the purpose of control and supervision provided in this Resolution, it is understood as intelligence the activity that aims obtaining and analyzing data and information producing and disseminating knowledge, inside and outside the national territory, regarding facts and situations of immediate or potential influence on the decision-making process, governmental action, safeguarding and security of society and the State (Paragraph 6). Meanwhile, for the purposes of control and supervision provided in this Resolution, counterintelligence is understood as the activity that aims to prevent, detect, obstruct and neutralize adverse intelligence and actions of any nature that constitute a threat to the safeguarding of data, information and knowledge of interest to the security of society and the State, […] (Paragraph 7, Resolution n.2 of 2013, Brazilian Congress).

institutions that are not part of the SISBIN system. All the same, to achieve the legislative control, the CCAI Commission could access files and infrastructures from SISBIN regardless of the degree of secrecy (paragraph 4). In this case, access to secret areas and facilities must be previously informed to the respective organizations and should preserve the protection of sensitive information and materials (paragraph 5).

To exercise the legislative control, the CCAI has the following missions: To examine and make suggestions to the National Intelligence Policy set by the President of the Republic; to make legislative proposals related to intelligence and counterintelligence activities. Moreover, the CCAI should elaborate on studies on the activity of intelligence; assessing the activities and functioning of the organs of SISBIN following the National Intelligence Policy. The legislative Commission should present recommendations to the Executive Branch in order to improve the functioning of SISBIN, monitoring the elaboration and dissemination of the National Doctrine of Intelligence, and supervise the curricular programs of the Intelligence School of the Brazilian Intelligence Agency (ESINT/ABIN) (section II of the same Resolution).

Furthermore, the CCAI has important roles concerning the legitimacy and efficiency of the intelligence community. For example, the Commission is able to receive and investigate complaints about violations of fundamental rights in the performance of intelligence and counterintelligence activities. Any citizen, political party, and association can present those complaints (item XI, section II). Yet, as we will show in this section, this ability has not been performed by the Commission in recent years. Notwithstanding, the Resolution enables an important power to the CCAI that could be developed in case of fundamental rights violations by intelligence. In that case, this capacity would be similar to the mission of Ombudsman bodies that oversee intelligence services in countries such as Canada and Australia (Gonçalves, 2008).

Another important power of the CCAI relates to the capacity to control the budget of intelligence and counterintelligence organizations at the federal level (item XII, section II, Chapter 1). The Commission can present amendments to the preliminary report of the annual budget bill, including proposals of additional credits destined to the costing and expenditures of SISBIN activities and programs. Therefore, the Commission has similar functions to the Spanish Commission to Reserved Credits that controls the CNI. However, this competence is still being improved in Brazil as the Congress Commission of Budgets rejected the amendments presented by the CCAI to alter the budget for intelligence in the recent years (we will address the history of the Commissions in the next pages).

In case the Executive dodges the control of CCAI, the final dispositions from Section II of the Resolution 2 of 2013 mention that “the unjustified refusal to

provide the information required [by the Commission], within the constitutional term, by the authority cited in the caput of this article, implies in a crime of responsibility". To avoid dilemmas related to the disclosing of information based on national security reasons, the Resolution expresses that "confidential classification of information or secrecy for the security of society and the state shall not be considered as justifications for the non-provision of the same information, within the constitutional term". This point is essential insofar as the CAAI has the power to request information despite any level of classification and secrecy. Thus, the Legislative control, at least from the legal point of view, should prevail in case of clashes between the Congress and the Executive regarding the accountability of classified matters. If the Executive seeks legitimacy and wants to demonstrate efficiency, then the Parliament must be able to assess sensitive information in a horizontal relationship where the *potestas* of the former should not hamper the controlling tasks of the latter. In that sense, the CCAI is also responsible for convoking "Ministers of State, or members directly subordinated to the President of the Republic, to personally provide information on matters of intelligence and counterintelligence preserving the rituals of secrecy and confidentiality" (Art. 5, section II, Chapter 1). Moreover, the Congress Resolution allows the CCAI to convoke other persons in the accountable actions, aside from the GSI Chief. Art. 6 defines that "the CCAI could invite any authority or citizen to provide clarification on matters related to the activity of intelligence, counterintelligence, and safeguarding of information". This mechanism was especially used to invite academics and other intelligence representatives (as from the Federal Police and ABIN sub-units) to give accounts about operations in the last years. In our vision, since the SISBIN is a huge intelligence system comprised of many organizations, it seems reasonable to enact the CCAI with powers to call different directors and professionals linked to the system. Moreover, despite the GSI Chief authority to command the SISBIN, he/she could not be able to know all the variables and complexity of the system as inferior ranks. The hierarchy does not necessarily translate the flow of knowledge in the System. Besides, the discretional ability of lower ranks is an important source that must be incorporated to maximize the accountability to the Parliament.

Now we turn to the composition and functions of the Mixed Commission for the Control of Intelligence Activities (CCAI). As expressed by Chapter II of the Resolution n. 2 of 2013, the Commission is comprised by the Presidents of the Committee on Foreign Relations and National Defense in the House of Deputies and the Federal Senate, by the Leaders of Majority and Minority groups in the House of Deputies and the Federal Senate, and by six members elected for a term of two years (renovation of the term is permitted).[49] The Commission has

[49] a) a Deputy appointed by the Leadership of the Majority of the Chamber of Deputies; b) a Deputy appointed by the Minority Leadership of the Chamber of Deputies; c) a Senator appointed by the Federal Senate Majority Leadership; d) a Senator appointed by the Minority Leadership of the

permanent advice from consultants of both legislative Houses that, by the designation of the Commission, might have access to the information and facilities expressed in Article 2 of the Resolution. In terms of functioning, the CCAI works by the decision of the President of the Commission and the measures can be reviewed by any of the members of the Commission in the following five regular meetings. If included in the agenda, the reviewing act is discussed and voted in a single session (paragraph 3, section II, Chapter II).

To institutionalize the activities of the Commission, Chapter IV defines that the Executive Power might send partial reports regarding intelligence and counterintelligence activities developed by the SISBIN every six months. In addition, the Executive is obliged to show a general and consolidated report of the intelligence and counterintelligence activities every year. However, exceptional reports and inspections could be requested at any time by the CCAI. In the CCAI meetings, the reports are classified as secrets because "their treatment and handling attach to legal and regimental rules regarding classified classification and safeguards of confidential matters" (Paragraph 10, section VI, Chapter II).

The Resolution also specifies the kind of information that the Congress Commission is able to obtain from intelligence services. The CCAI could request partial and general information regarding the:

> I - indication, structure, and strategy of the organization or entity involved in the activities of intelligence, counterintelligence, and safeguarding of confidential matters;
>
> II - history of the activities developed and its relation with the National Intelligence Policy, the action strategy, and the operational guidelines;
>
> III - list of the organizations that cooperate with the SISBIN as well as the entities who maintain links and joint actions with this system;
>
> IV - list of all foreign intelligence or counterintelligence agencies that have acted in cooperation or that have provided any type of advice or information to a Brazilian intelligence body or entity;
>
> V -identification of processes used to carry out intelligence and counterintelligence activities, and safeguarding of confidential information;
>
> VI - a detailed description of the amounts allocated and the expenses involved in carrying out the activities of intelligence, counterintelligence, and safeguarding of information. (Paragraph 10)

Federal Senate; e) a deputy appointed by the Committee on Foreign Relations and National Defense of the Chamber of Deputies, by secret indication from its members; f) a Senator appointed by the Foreign Affairs and National Defense Committee of the Federal Senate, by secret indication from its members (art. 1, section I, Chapter II, Resolution n. 2, 2013 Brazilian Congress).

The above terms are the guidelines that intelligence reports must contain when delivered to the CCAI. Despite the terms "indication, structure and strategy of action" does not necessarily correspond to operations and methods used by intelligence services, the point I define a basic set of actions that are complemented by points II (history of activities) and III (intelligence cooperation). In this latter point, domestic and international links are to be related to the Commission. Unlike Spanish Law 11/2002 that does not allow the Parliament to consult information related to the cooperation between Spanish and foreign services, the Brazilian text enables the National Congress to request this kind of information. The aim of this point could be related to the national interest of Brazilian representatives to assure that domestic intelligence is not coopted by stronger foreign services. Yet, this point could serve as a mechanism that enhances legitimacy and transparency alongside the activities developed with other countries, as in the case of the mega sports events such as the FIFA World Cup in 2014 and the Olympic Games in 2016. In those events, the ABIN received collaboration from international agencies as we will discuss below. Finally, the last points of the Resolution express that the reports must contain an economic history of the intelligence actions in order to facilitate Congress supervision. In that sense, Article 12 of Section II mentions that "the reports addressed in this article shall include the total amount of resources allocated and used in the execution of intelligence and counterintelligence activities, as well as in the safeguarding of confidential matters."

Yet, Article 13 defines that the CCAI will produce annual reports based on the accountability of the SISBIN to the National Congress. Those public reports must not include, at any circumstance,

> I - information that endangers the interests and security of the nation, the state, and society, or information that violates the intimacy, privacy, honor and image of persons;
>
> II - names of persons engaged in the activities of intelligence, counterintelligence, and safeguarding of information;
>
> III - intelligence methods used or sources of information to formulate the reports;
>
> IV - the amount of resources allocated and used specifically in each intelligence, counterintelligence, and information safeguarding activity.

The censorship expressed above is expected since no intelligence service in the world reveals, discloses, or publishes details about their activities. Thus, the CCAI might access but never disclose intelligence information to the public. However, in case the CCAI understands that, for some reason, classified information from the SISBIN should be published, the legislators must inform the chief authority of intelligence to decide on the disclosing or alteration of the information (paragraph XII, same section). In that sense, the Commission is able to initiate a process of disclosing information, but the intelligence authority or the

superior hierarchical authority (in this case, the GSI Chief) has important veto power. In the case of Spain, this process is more complex since the classification of some information (secret and reserved) is decided by the Council of Ministers that enclosed it. In Brazil, different authorities can be involved in this decision, but the GSI Chief has preeminence in case the information relates to intelligence activities within the SISBIN system. We will return to this topic in the judicial control.

Chapter V of the Resolution also establishes specific procedures for the legislative control of intelligence activities. According to Article 14, members of the Commission, consultants working with the CCAI, and persons engaged by contract, or by any other means to perform services for the CCAI, have access to classified information according to the level of secrecy (maximum security for ultra-secret, and minimum security for secret) and by using specific security credentials and authorization. Article 15 mentions that those persons should not release information that violates privacy, private life, honor and the reputation of individuals. The release of information considered as a threat to national security, under the deliberation of the majority of the Commission, is also prohibited. This article gives the impression that the Commission has certain leeway to decide upon the disclosure of confidential information based on internal deliberation. Yet, we need to remember that intelligence services would offer information that Congress members request in advance. In that case, the former can exercise denial of information or guide the access according to its preferences. Thus, despite the good intentions of the legislation, it seems that on rare occasions the Commission will be able to decide upon disclosing and revealing secrets. Moreover, the mentioned *potestas* or veto power of intelligence authorities constitutes another obstacle to disclose information.

There are also rules for requesting information by the CCAI that need to be justified by the members, as well as explained to the Plenary of the Commission before they are included in the regular agenda. Thus, the Brazilian Commission works in the base of proposals, amends, and votes the topics that will be discussed in the next sessions. The same process could be adopted to decide whether the sessions are held behind closed doors, with no access from external members and public, as in the case in which the GSI Chief or the ABIN director are called to give accounts of their actions (Article 22). The Resolution also defines that the CCAI sessions are to be held every month on a regular base, except when the Committee decides otherwise. As we will see, this obligation was not followed in recent years. Besides, the internal and external communications, as well as the reports and documents produced by the CCAI constitute reserved information unless the majority of the Commission decides to publish them (Article 25). Finally, the CCAI could visit SISBIN locations and facilities in order to have access to specific information that is preserved by specific rules of restricted access. The Commission also can demand to have a specific room or place to store secret

documents, avoiding the removal or transportation of files, even for inspection, from the places they are stored (Article 27).

In light of the above, the Brazilian Congress Resolution is more extensive when it comes to rule the Legislative control of the intelligence system than in Spain (Law 11/1995). It seems that the Brazilian Resolution tried to fill the normative gap between the creation of the SISBIN in 1999 and its promulgation in 2013. The Resolutions also tried to "catch up" with the norms from other countries to oversee this kind of secret activities. If the delay was the negative point, the good part is that the resolution is extensive in some aspects to enhance a completer and stable control in the hands of the CCAI. Yet, in practice, there were no substantial modifications in the role of the Congress to tame the secret services. We will explain this performance below. Before, let us turn to a final proposal that can affect the legislative control of intelligence in this country.

Since the first intelligence norms were enacted more than ten years after the Constitution, law proposals such as Bill N. 67 of 2012 aimed to put the intelligence activity among the core actions of the state by inserting an amend on the fundamental titles of the Constitution. This proposal can be understood as an attempt by intelligence officials to consolidate their roles as watchers of the state from a legal perspective. By Bill N. 67 of 2012, intelligence would be elevated to the constitutional level to avoid institutional setbacks and substantial reforms by the Congress. In terms of the legislative control, the proposal aimed to define that "the external control and oversight of the intelligence activity shall be exercised by the Legislative Branch, especially through an external control body composed of Deputies and Senators, and with the assistance of the National Intelligence Control Council" (art. 144, E). In other words, besides the mentioned Mixed Commission for the Control of Intelligence Activities (CCAI), this proposal tried to enact a Council as an auxiliary organ of external control of the Legislative Branch composed of nine members. These members were to be chosen among Brazilian citizens with technical knowledge or experience regarding the final control of intelligence. In this model, the following composition was expected: three members indicated by the Federal Senate; three by the House of Deputies; one by the President of the Republic; one by the National Council of Justice; one by the National Council of Public Prosecutions. The Directors would have a term of five years renewed once, and would be dismissed only by decision of the National Congress, under the proposal of the control body or vote of one-fifth of the members in each House. According to their authors, the Council and the Commission should have full access to the information and knowledge produced by the intelligence services, preserving their confidential nature.

The Bill was archived in December of 2018. However, it brought up the idea of an auxiliary body to complement the role of the Congress Commission. This model, adopted by countries like Canada, enhances a network of accountability

which combines political boards (as in the case of the Commission) and technical expertise (Council) to improve the control and oversight of the intelligence and counter-intelligence activities. Naturally, the implementation and coordination between those bodies are matters for speculation. For instance, the creation of a parallel body can either improve or hamper intelligence collaboration and submission to external controls. It is known that intelligence services use to be cautious when they disclose information according to the political moment and situation of the Houses, such as parliamentary groups and opposition parties that are not only interested in controlling this activity. Thus, a technical Council might balance the self-restraining effect of intelligence when supplying accounts to external entities. However, a technical body does not imply necessarily political neutrality and the best assessment of the secret services. This group can work as veto power or create blind spots for the strengthening of accountability actions, especially when they are indicated by the Executive branch itself. In any case, deeper and completer actions are welcome if they improve the answerability and responses of the intelligence system before external commissions or bodies.

Now we address the main events and sessions that marked the history of the legislative control. We will follow two steps to analyze this kind of control in Brazil. In the first step, there are no official records of the sessions from 1999, when the ABIN-SISBIN was created, to 2013. Thus, we will use specific bibliography produced by scholars or researchers that have already addressed this topic. In the second step, from 2013, when the CCAI was regulated, to 2019, we directly use the documents and database available by the Senate and House of Deputies in order to reconstruct the sessions of the Commission (See Annex II in Appendices).

When Law 9.883 of 1999 created the SISBIN and ABIN, the first Commission for Control of Intelligence Activities took place in November 2000 (11 meetings were held between November 2000 and July 2004). The first meeting of the Commission, formerly known as the External Control and Inspection Body of the National Intelligence Policy (OCFEPNI), was held due to scandals disclosed by the press in which the ABIN was illegally spying national political figures, journalists, attorneys, and social movements during the late 1990s (Antunes, 2004). After these events, General Alberto Cardoso, Chief Minister of the Cabinet of Institutional Security (GIS), publicly requested the President of the Senate, Antônio Carlos Magalhães, to install the Commission. The General assumed and recognized the accusations during this meeting, and the members declared their upset because the motive of the meeting was caused by political scandals. Thus, they stressed the need to be more deeply involved in the control of this subject. According to Antunes (2004), the only effective action of this meeting was to request Minister Alberto Cardoso to report on the activities carried out by the ABIN since its creation in 1999.

The second meeting was held in November of 2000 when the Commission scrutinized General Alberto Cardoso and the ABIN Director, Colonel Ariel de Cunto, in a secret meeting. Although secret, the session counted with 10 deputies that were not members of the Commission. According to an interview with General Alberto Cardoso given to Antunes (2004) in August 2002, the presence of those members caused the general to restrain his presentation, reducing the information that could have been given to the Commission. This was only one example of the obstacles caused by the delay to approve the CCAI regulation.

The third meeting of the CCAI was held in August 2001. The meeting was called in May and June but did not happen due to the lack of quorum, attesting the lack of Legislative interest in this matter. In the meantime, ABIN's facilities and infrastructures were visited by the Commission following the invitation of General Alberto Cardoso. After this event, the psychologist Marisa Del 'Isola Diniz was approved as the ABIN Director. The fourth meeting of the CCAI was held in November 2001. The event was scheduled for August 22 and October 24, but it was delayed due to the lack of quorum. At this session, Deputy Luiz Carlos Hauly and Senator Eduardo Suplicy made proposals to regulate the legislative control of the ABIN. However, their actions were not approved in the Plenary. During the sessions, the representatives debated the National Policy Intelligence. Senator Pedro Simon's first amendment addressed the need for defining the areas in which intelligence should, in his view, be prohibited from acting such as for political, religious, and sexual reasons. The proposal passed and was accepted. Meanwhile, other amendments were sent by Senator Heloísa Helena and Deputy Aloízio Mercadante. They proposed that the ABIN objectives should only be compatible with Human Rights and with the guidelines formulated by the external control body. The proposals were rejected because the Commission believed they exceeded the functions and jurisdiction of the Congress, which was supposed to send suggestions regarding the intelligence policy and to act following Law 9.883/1999.

In 2002, the first meeting was held to clarify the alleged ABIN surveillance over Governor Roseana Sarney, considered by opinion polls as a strong candidate to run for the federal elections. According to Antunes (2004), the CCAI decided to invite General Alberto Cardoso to explain this case. The second part of the session was dedicated to analyze the social Landless Movement (MST) actions, such as the invasion of a farm owned by the President Fernando Henrique Cardoso. The commission complained that the agency was unable to warn the president about the imminent invasion.

Considering the first years of the legislative activity, Antunes is very sharp in her words to assess the work of those commissions:

> At the risk of being unfair with some of them, the work of the Members of the Parliament can be summarized to the elaboration of questions

> that have been influenced by the press. When intelligence officials answer those questions, they [the MPs] tend to be satisfied with vague responses and counter-arguments that are usually offered to induce a sense of normality and transparency. MPs were even naive in believing certain responses emitted during these debates. For example, when a member of the Federal Police, Getúlio Bezerra dos Santos, was asked about the counterpart that the Police provided to the US government in exchange of US $ 3.5 million sent by Washington each year, he replied: "nothing". Then, the question was considered as fully answered by the Commission. Other MP replied that the US money should have been transferred to the United Nations and poor countries (Antunes, 2004, pág. 34).

If the quotation is correct, it attests how the Congress representatives were unaware of the mechanisms that ruled the activities of security agencies. The lack of expertise was also observed in the next meeting, on June 2002, when General Alberto Cardoso and the Minister of the Superior Electoral Court were invited to speak about the ABIN participation on the Center for Research and Development (CEPESC) in the context of the national elections in 2002. Before this meeting, the media questioned if it was pertinent to assign the ABIN as responsible for the protection of electronic data and as the unique agency to have access to the cryptography of the electronic ballot boxes. Another session occurred in the same month. We do not have information about the contents of this secret meeting in which the GSI Chief Minister, General Alberto Cardoso, and the Director of the Federal Police, Itanor Neves Carneiro, spoke about the public security situation of the country.

In 2003, the Presidency of Luis Inacio Lula da Silva did not change the reactive roles of Parliamentary Commissions in matters of defense and intelligence. In 2003, Senator Eduardo Suplicy assumed the Chair of the Commission but there were no meetings during this year. One meeting would have happened on April in exceptional circumstances to hear the former head of the Federal Bureau of Investigation (FBI), Carlos Alberto Costa, to clarify his statement in *Carta Capital* magazine in which he assumed that the American enforcement agency coopted the Federal Brazilian Police with money to fight drug trafficking and organized crime. However, no information was found about this testimony. This year, according to *Estado de Minas* and *Correio Brasiliense* newspapers, [50] the government expressed concern because many factions were clashing to take control of the ABIN from within. According to these sources, the leadership was disputed among civilian and military remnants of the former SNI (National Information Service), freemasons and newly hired agents of ABIN, and by a group that would be formed by representatives of all those factions that called themselves "union section".

[50] Figueiredo, L. 2004, July 4th. 'Crise na Abin: Espiões fora de controle'. *Jornal Estado de Minas*.

During the first years of Lula administration, Antunes (2004) evaluates the Commission and criticizes the fact that the Commission was not able to approve its internal regulation. Consequently, the Commission operated without a permanent structure and with few representatives. Moreover, to her, the inefficient functioning of the Commission was explained because party leaders accumulated several tasks in the National Congress. Besides, few politicians were interested in intelligence matters. In other words, during the first years of the Commission, the Legislature abandoned its role to improve and to turn more accountable the Brazilian Intelligence System.

In 2005, the ABIN and the GSI needed to clarify news in which, according to *Veja* magazine, the agency reported that the Workers Party (PT) received campaign donations in 2002 from the Revolutionary Armed Forces of Colombia (FARC).[51] The Commission produced a secret report, followed by the release of a note explaining that the news was false. Only two sessions were held in 2006 whereas in 2007 there were none. No references and reports were found for the meeting in 2006. In 2008, the GSI Chief Minister was summoned to clarify, in a secret session, the robbery of computers containing sensitive data of Petrobras, the state-sponsored Oil Company that years later was the center of major corruption scandals. Yet, it is no possible to establish a correlation between those episodes. In a new meeting in 2008, the GSI Chief Minister was called again to clarify the operations of the Army in the favela Morro da Providência in Rio de Janeiro (Gonçalves, 2010). The episode refers to the participation of the Armed Forces in a social project called "Social Cement" (*Cimento Social*) with support from the Mayor of the city, Marcelo Crivela. During this event, soldiers would have kidnapped David da Silva, Wellington Ferreira, and Marcos Campos. Those young people would have been "delivered" to rival gangsters that tortured and executed them.[52]

Later in 2008, a series of public and secret hearings were held to investigate the involvement of an intelligence network that supported the so-called Operation Satiagraha, an action conducted by the Federal Police Department to investigate crimes against the Brazilian financial system. According to Carpentieri (2016), telephone calls between the president of the Supreme Federal Court (STF), Gilmar Mendes, and senator Demosthenes Torres were leaked during the investigation. This was a piece of evidence that the ABIN was monitoring the STF magistrate. In September, the GSI chief minister, the ABIN director-general, and the Federal Police Director were all convoked by the Commission. At the request of the GSI, the Technical-Scientific Directorate of the National Institute of Criminalistics of the Federal Police sent a report on 16 equipment used for scanning and monitoring targeted people. This report concluded that the ABIN did not have the capacity for

[51] Azevedo, R. 2005, March 16th. `'Os tentáculos das FARC no Brasil'. *Veja*.
[52] Naddeo, A. 2008, June 17th. Saiba quem eram os três jovens do morro da Providência mortos no fim de semana. Uol Notícias - Cotidiano. Retrieved from: https://noticias.uol.com.br/cotidiano/2008/06/17/ult5772u120.jhtm in 10/12/2019.

spying cellphone signals. However, the reports of the Federal Police and the ABIN presented some contradictions. In the end, it was discovered that lower-ranked police officers allowed intelligence agents to participate in criminal investigations without the knowledge of the Federal Police directors. Eventually, this tactic served as a legal base to the cancellation of the judicial process against major banker figures such as Daniel Dantas. The impact of the Satiagraha Operation served to debate the use of intelligence agents to interfere with police investigations and the ability to conduct enforcement activities. This point will be addressed in the judicial control of intelligence (Section 3.6 in this Chapter).

Between 2009 and 2012, no report was found for the Commission. Carpentieri (2016) infers that this period of inactivity lasted until 2013 when the aforementioned National Congress Resolution No. 2/2013 of the National Congress finally regulated the work of the Congress. After the regulation, the number of members increased from six to thirteen members. Meanwhile, the Commission scheduled monthly meetings to demand SISBIN partial reports and general reports. Extraordinary reports would have been requested at any time, but the control focused on SISBIN organizations at the federal level. Thus, there are no legal grounds to oversee intelligence agencies at other federal levels such as states and municipalities.

After 2014, we use the Senate and the House of Deputies databases to reconstruct the Commission meetings. This year, on March 19, the first CCAI meeting was held to define the President of the Commission. The second meeting happened on April 22, and the goal was to define the schedule of the Commission. The session had reserved access according to the art. 22 of Resolution no. 2, 2013 of National Congress. On May 21, a third meeting was held to define the schedule but the session was also secret. At the times of this event, General José Joselito, the GSI Chief, was convoked to clarify the alignment between the Landless Social Movement (MST) and the Venezuelan government, as alleged by *O Globo* newspaper.[53] The author of the initiative was Representative Domingos Savio from the Brazilian Social Democracy Party (PSDB). The request was approved but since there was no sufficient quorum, the initiative did not pass and remained excluded from the secret session held with the GSI Chief. On November 11, a fourth meeting had the objective to set the agenda of the CCAI and Domingos Savio initiatives to clarify the links between the MST and the Colombian FARC did not pass due to the lack of quorum. On November 18, a session that was scheduled based on art. 22 of

[53] *O Globo.* 2014, November 03rd. 'Governo venezuelano assina convênio com o MST'. Retrieved from: https://oglobo.globo.com/brasil/governo-venezuelano-assina-convenio-com-mst-14452866 in 10/12/2019.; see also: Passarinho, N. 2014, November, 05th. 'Comissão quer ouvir ministro sobre convênio entre MST e Venezuela'. *G1 Política*. Retrieved from: http://g1.globo.com/politica/noticia/2014/11/comissao-quer-ouvir-ministro-sobre-convenio-entre-mst-e-venezuela.html in 10/12/2019.

Resolution N.2 from 2013 was not held by the Commission. On November 25, a new meeting was canceled.

In 2015, on April 9, the first meeting of the year aimed to include proposals of CCAI members. On April 28, the proposals were discussed in a deliberative session. The president of the Commission, Representative Jô Moraes from the Brazilian Communist Party (PCdoB), proposed to visit the buildings of the ABIN, the Department of Intelligence of the Ministry of Defense, the Intelligence Centers of the Armed Forces, and the Police Intelligence Directorate of the Federal Police. Senator Aloysio Nunes from PSDB proposed to convoke the GSI Chief, General José Elito when the newspaper *Estadao* newspaper denounced that the Islamic State (ISIS) was about to recruit young Brazilian people.[54] Nunes also requested clarifications to alleged infiltration of Cuban agents in the Medical Cooperation agreement (*Mais Médicos*) between Cuba and Brazil. The proposals were accepted in the deliberative session.

On May 05, 2015, the Commission received the GSI Chief Minister, General José Elito. Whereas the first part of the session was public, the second one was held in secret. During the first part, General José Elito explained the work developed by the SISBIN and ABIN, mentioning the Mosaic System in which the security agencies created different scenarios to carry on their activities. As mega sports events were about to happen in Brazil, he mentioned that the ABIN was analyzing and working in more than 700 security scenarios to protect athletes and delegations in a continental country like Brazil.

On July 7, 2015, the third meeting of this year was held to hear the proposals of the CCAI members. Through a deliberative process, the president of the Commission, Representative Jô Moraes proposed, proposed to organize the International Seminar entitled "Intelligence Activity in a Democratic State" in order to discuss intelligence in a democratic state and the competences of the Legislative power. She also proposed to assess intelligence regarding the mega-events held in Brazil during those years (the Military World Games, the Confederations Cup, the Youth World Day, the Football FIFA World Cup, and the 2016 Olympic and Paralympic Games). In that sense, she invoked again the GSI Chief Minister, General José Elito. The Commission approved the proposal and, on July 14, a public session was held with the General. In addition, more guests were convoked to discuss legislative reforms and intelligence during the Seminar. The guests were Denilson Feitoza Pacheco, president of the International Association for Security and Intelligence, Joanisval Brito Gonçalves, consultant of the Federal Senate specialized in Intelligence and Intelligence Control, and Edmar Furquim Cabral de Vasconcellos Junior, intelligence official and member of the ABIN. During the

[54] Castenheda, E.; Matais, A. 2015, March 21. 'Governo detecta recrutamento de jovens pelo Estado Islâmico'. *Estadao*. Retrieved from: https://internacional.estadao.com.br/noticias/geral,governo-detecta-recrutamento-de-jovens-pelo-estado-islamico,1655354 in 10/13/2019.

session, Denilson Feitoza complained about the delay to approve the National Intelligence Policy (PNI). Joanisval Brito insisted on the importance of intelligence as a key component of decision-making. For him, intelligence was valuable to different users, from a lieutenant commanding a border squad in the Amazon, to governors of the states, the President of the Republic, and CEOs of large companies. He also criticized the lack of legislation to define clear mandates to conduct telephone interceptions by the ABIN. To him, this capacity was important to monitor people that were suspects of foreign espionage and terrorism. "It is inconceivable that intelligence cannot access their communications", he told during the meeting.[55]

On August 08, 2015, the meeting had a deliberative session to include proposals and topics to the CCAI agenda. Senator Aloysio Nunes from PSDB proposed to invite the GSI Chief to explain the delay in the publication of the National Intelligence Policy (PNI). Meanwhile, Deputy Jô Moraes requested an overall assessment regarding the performance of the intelligence services during the mega sports events. The Commission approved both initiatives. The next meeting happened on October 6 with the participation of the GSI Chief Minister as well as of representatives of the National Association of Intelligence Officers (AOFI), and the Association of the Officials of the Brazilian Intelligence Agency (ASBIN) to discuss the proposals. On October 13, a new meeting was held to deliberate the amendments sent to the National Budget and Financial Plan (PLOA) in order to alter the funds of the intelligence service. The invited participants were Eduardo Paes (Mayor of Rio de Janeiro), William Murad (Intelligence Director of the Security Secretariat of mega-events), Wilson Trezza (Director of the ABIN), Colonel Marcelo Rodrigues (Counterintelligence of the military). The outcomes were 27 amendments, 26 proposals, and a text presented to the PLOA Commission. During the public session, Representative Heráclito Fortes, member of the Brazilian Social Party (PSB), inquired the ABIN Director regarding the "serious issue" represented by the illegal migration to the country (in the context of Haitian and South American waves of migrants going to Brazil). Whereas Wilson Trezza answered that the ABIN was conscious about this issue, he tried to emphasize the importance of intelligence to a country like Brazil to obtain more financial funds and political support of Legislators in the Commissions. He mentioned that the ABIN worked in apolitical and nonpartisan lines adopting the same procedures regardless of the political situation. In his words "the only thing that differentiates the Brazilian intelligence from the best intelligence in the world is adequate budget and legislation that supports the activity to access new technology". To him, legislators needed to strengthen the structure of intelligence, defense, and security in a country of 204 million inhabitants, the world's 7th economy, and with

[55] CCAI Commission data base and reports retrieved from the official website of the Federal Senate in Brazil. Retrieved from: https://legis.senado.leg.br/comissoes/comissao?0&codcol=449, accessed in 10/13/2019.

aspirations to have a seat in the UN Permanent Council of Security. However, the ABIN director did not make substantial comments when the Representative Heráclito Fortes inquired him about the institutional reform ti put the ABIN under the President of the Republic, rather than to the Cabinet of Institutional Security (GSI). One year later, a Presidential Decree of Dilma Rousseff extinguished the GSI. However, the previous institutional configuration was reestablished after the impeachment of Rousseff in 2016.

There is no evidence to confirm if the amendments to alter the credits for intelligence were accepted in that meeting. However, on October 15, 2015, another meeting was scheduled to propose more amendments to the Congress Commission on Budget and Financial Plans. Before that, the CAAI deliberated and approved the following four amendments: 1. Support of mega-events handled by the Ministry of Defense, the addition of R$ 30,000,000.00. 2. Stealthy actions of the Navy Command, the addition of R$ 10,000,000.00. 3. Technological Development of the Army, addition of R$ 20,000,000.00. 4. Intelligence Actions of the Brazilian Intelligence Agency - ABIN, the addition of R$ 60,000,000.00. The amendments were attached to a general justification to increase intelligence and security budgets, mentioning the importance of these activities to the country. However, the justifications lacked consistency and details regarding operations and sources that probably did not deserve classification. Despite the CAAI justifications, legislators from the Congress Commission on Budgets and Financial Plans rejected the amendments. The reasons that motivated the rejection were not clear.

On November 10, 2015, a new meeting was held to discuss the reform of the Brazilian intelligence legislation. The Commission requested the presence of Carlos Terra Estrela (President of the Association of Intelligence Servers), and Luciano Jorge (Vice-President Association of Intelligence Officials). In this meeting, Luciano Jorge expressed his concern about the Brazilian dependence on international actors to protect national communications through encryption and databases. He mentioned that Brazil had only one geostationary satellite. According to him, since the owner of the satellite was the Mexican magnate Carlos Slim, this person had sovereignty do decide upon Brazilian communications, from WhatsApp messages to cellphone calls. Nevertheless, the electrical and signal capacity of Brazilian communications does not depend entirely on that satellite. For example, telecommunications are amidst the governance of several companies and IP providers. Besides, most of the internet communication is also based on optical fiber cables that cross the country. In that sense, it seems that Luciano Jorge exaggerated his statement to justify the financial amendments to improve electronic intelligence capacities. Hence, because of their technical expertise, some intelligence agents might express unchecked information that could be considered as reliable by unaware representatives who oversee this activity.

On May 31, 2016, the Commission convoked the Chief Minister of the Institutional Security Cabinet (GSI), General Sergio Westphalen Etchegoyen. The meeting was held in secret and there are no records of this session. Another meeting was scheduled for June 28. This session aimed to propose amendments to the Commission nº 2, of 2016 to alter the credits and budget of the intelligence service. Deputy Pedro Vilela was the coordinator of the amendments. However, the meeting was canceled and postponed to October 18. The inactivity of the Commission probably resulted from the political turmoil caused by the impeachment of Dilma Rousseff and the promotion of the Vice-President Michel Temer to the Presidency of the country. The Commission tried again to approve the following four measures to alter the national budget: 1) Army Command Budget Unit, Action 147F - System Deployment of Cyber Defense for National Defense, the addition of R$ 70,000,000.00. 2) Unit Budgetary Command of the Navy, Action 2866 - Shares of Secret Character, the addition of R$ 1,000,000.00; 3) Budget Unit for the Brazilian Intelligence Agency, Action 2684 - Intelligence Actions, the addition of R$ 10,000,000.00. 4) Budget Unit for the Federal Police Department, Action 15F9 - Institutional Improvement, the addition of R$ 80,000,000.00. Notwithstanding, the Congress Commission on Budgets and Financial Plans rejected again the CCAI amendments as the financial crisis of the country increased during that fiscal year. On November 29, another meeting was held with the presence of the GSI Chief, General Sergio Westphalen Etchegoyen. As the session was conducted under secrecy, thus, there are no records and data.

On April 03, 2017, the CCAI elected Bruna Furlan as President of the Commission, and the Senator and former President of the Republic, Fernando Collor, as the Vice-President of the Commission. On October 19, another meeting aimed to make budget amendments to expand the intelligence funds. Furthermore, the CCAI members discussed proposals regarding the National Defense Policy, the National Defense Strategy, and the White Book on National Defense. Whereas the amendments to increase the budgets of intelligence were approved in public deliberation, General Sergio Westphalen Etchegoyen answered inquiries in a secret session held behind closed doors. After the internal deliberation and the secret session, the budget amendments were rejected by the Congress Commission on Budgets and Financial Plans once again.

Finally, on October 18, 2018, in the only reported meeting of that year, the CCAI approved the following amendments: Amendment 1: Budget Unit 52,121 - Army Command, Program 2058 - National Defense, Action 147F - Implementation of Systems of Cyber Defense and National Defense, the addition of R$ 70,000,000.00. Amendment 2: Budget Unit 52,131 - Navy Command, Program 2108 - Management and Maintenance Program of the Ministry of Defense, Action 2866 - Shares of Secret Characteristics, the addition of R$ 5,000,000. Amendment 3: Budget Unit 52,111 - Aeronautics Command, Program 2108 - Program for the Management and Maintenance of Ministry of Defense, Action 2866 - Shares of

Secret Character, the addition of R$ 20,000,000. Amendment 4: Budget Unit 20,118 - Brazilian Intelligence Agency, Program 2101 - Management and Maintenance Program of the Presidency of the Republic, Action 2684 - Intelligence Actions, the addition of R$ 80,000,000.00. In this case, we have not found reports regarding the destination of the amendments after they were approved by the CCAI.

Those are the main events and meetings of the Commission for the Control of Intelligence Activities in Brazil during the last years. If we consider the official database as an indicator of the frequency of the meetings, it is noticeable that the number of sessions has sharply diminished since the Presidency of Michel Temer. We do not know exactly the motives, but this could be a symptom of the lack of interest of the new legislators to control the intelligence service, especially after many of the budget proposals of the CCAI were rejected in subsequent Congress Commissions. On the one hand, the CCAI specialized itself in proposing amendments to increase the intelligence budget as a consequence of the election of representatives aligned with security institutions and doctrines (as in the case of police officers and military that became Deputies and Senators). This alignment could be related to the GSI reinforcement after a short extinction in 2016 and to the creation of the Intelligence National Policy in 2017 by the new government. Both actions can be inserted in a context of new militarization promoted by the President that might have been echoed by the legislators. In that sense, the Commission acted as a corporatist front aligned with security demands, rather than as external control body of the intelligence activity. On the other hand, even if representatives were not necessarily coopted by the Executive or intelligence interests because they already had a "security and intelligence" mentality, it remains unclear why the Resolution N. 2 of the National Congress of 2013, which established monthly sessions and annual reports of the SISBIN system, was not implemented in the recent years. Moreover, most of the meetings and sessions during the last decade simply did not follow the parameters and motivations that legislators should take into account to request classified information from the secret services. It seems that the basic mechanism applied in those sessions was inviting key figures, such as the GSI Chiefs, and just receiving vague explanations about particular events (i.e. sports events, scandals leaked by the press, etc.). Despite the advances brought by the Resolution to control and oversee the intelligence activity, this effort has not been institutionalized and still can be developed in this country.

Epilogue

The ability to establish legislative controls over intelligence agencies in Spain and Brazil is far from being satisfactory. Why does this happen? To answer this, we will depict some theoretical insights that might explain some of the macro-dimensions attached to legislative bureaucracies and security institutions. Those insights, in turn, could shed light upon the limitations of this kind of control in the case studies. The theoretical insights stem from two acknowledged women scholars in this field: Amy Zegart by her seminal work on the institutional configuration of the security community in the United States; and Marina Caparini by her overall research about the oversight of intelligence.

According to Zegart (2000), the institutionalist design to define the importance of the rules of the game and the rationality to make decisions are not equally distributed between the various branches of the state bureaucracy. On security, politics has less distributive characteristics as interest and advocacy groups are weaker and historically more recent when compared to other groups, such as labor and industry. In addition, information about the performance of government agencies related to institutional security is much less widespread due to the secrecy of some activities and the heavy safekeeping requirements to protect it. Besides, the Executive predominates and, traditionally, the Legislative had less activism or mobilization in this area. Finally, Zegart expresses the difficulty of establishing jurisdictional limits of action due to the interdependence between these bureaucracies: armed forces, chancelleries, intelligence agencies, and security forces. These organizations have higher levels of interdependence than domestic bureaucracies (education, health, transportations, etc.). Zegart set of factors would discourage the participation of the Legislative in the design and supervision of agencies linked to institutional security. Hence, Zegart's thesis argues that bureaucracies in this area tend to be created by the Executive (with the secondary and always reluctant role of the Legislative). Moreover, the choices about organizational designs and initial rules reflect the institutional disputes between sectors of the bureaucracy within the executive branch, with the legislature exercising a kind of unsystematic and ineffective supervision.

Written to the American security community in the late 20th century, Zegart's words are very insightful to our cases. As seen in this section, the dynamics of governance in the field of security are very restricted, both in terms of plurality and in terms of actors. Also, the legislative commissions tend to be hijacked by the information disclosed by the government, requiring a greater involvement of representatives, researchers, and civil society. In the case of intelligence activity, the challenge is even greater. Recognizing intelligence as legitimate and necessary is a hard issue, especially in cases that have emerged from authoritarian periods with no involvement of the Parliament in the Executive agenda. Moreover, the efficiency of the Commissions does not increase the

reputation of representatives, nor it produces direct electoral benefits. Besides, there is a lack of expertise and technical involvement to request information from the government. Those factors produce a scenario where the Legislative has no incentives to establish efficient and permanent controls over intelligence.

According to the second scholar, Caparini (2016), the expenditures for intelligence services are often embedded deeply in a government's overall budget, as in the case of the Spanish Reserved Fund, and, in practical terms, "many parliaments exercise little scrutiny of the intelligence budget" (Caparini, 2016, p. 20). In a similar way, Parliamentary Commissions can be ineffective receiving insufficient knowledge of the work performed by the agency. Lack of expertise often is the result when legislative members do not acquire long experience on committees, and this is important since many of the representatives are not reelected or at least do not have mandates comparable to the evolution of a state policies such as intelligence. Another phenomenon that prevents a legislature from functioning effectively as a mechanism of oversight for intelligence and security agencies is political deference found in parliamentary systems with a fused executive and legislative branch. In contrast to a presidential system of government where there is a separation of powers between Executive and Legislative branches and a system of checks and balances, in the Parliamentary system, the Executive is drawn from the legislature and power is unified or fused. Since the executive is accountable to the legislature, party discipline should be strictly maintained. Political deference may have a significant influence on the functioning of parliamentary committees, where members of the majority or coalition governing party are "unwilling to criticize the Prime Minister and the domains under his/her management" (Caparini, 2016, p. 23).

Zegart and Caparini's ideas are verified to a certain extent in Spain, where the scrutiny of intelligence has been historically scarce until the creation of the CNI in 2002, and even nowadays. In Brazil, a presidential system, the problem is that the opposition has been inexpressive to exercise a front of scrutiny. Moreover, the opposition depended on the colligation with several groups in a very heterogeneous and fragmented partisan scenario. Yet, because of the differences in the formation of the Executive, when compared to Brazil, the case of Spain is more notorious in the so-called capture of "iron triangles" of the government, especially in the first years of the CNI. The capture occurs when the controllers are too close to the institutional goals and problems of the controlled agency, resulting in "lower levels of independence and critical distance to accomplish an effective oversight" (Caparini, 2016, p. 4). In Spain, the capture was mitigated since the emergence of new political groups in the middle 2010s, implying in a new balance of forces between leftists and right-wing parties, as well as between centralist and nationalist groups to control intelligence. However, even Brazil has emulated the capture of "iron triangles" during the last years, as the legislative commission

echoed the militarization and preferences of the Executive to increase the budget of security agencies without a deep evaluation.

Now, let us summarize the main aspects of the Commissions in both of the countries and formulate overall recommendations.

In Spain, Law 11/1995 for the control of reserved funds allows parliamentary groups, representing at least one-quarter of the House, to request information on classified information through the Presidency of the Parliament. In addition, Resolution of the Presidency of the Congress of Deputies, of May 11, 2004, allows different criteria to disclose information categorized as secret or reserved to the Parliament. The Executive could provide information on a certain matter declared as secret exclusively to the President of the Congress or the President of the Commission. Furthermore, the Executive uses to provide reserved information in closed sessions. In that case, only members of the Commission are allowed in the sessions.

Since Parliament members usually do not know internal procedures and protocols of intelligence, the control of the CNI depended on the very predisposition of this agency to be controlled. This reminds the asymmetry of power in accountable actions analyzed in the theoretical part (see section 1.4), a situation in which the accountant actor dictates the agenda and the topics of the accounting action. Another obstacle is that classified information is regulated by the Council of Ministers. In this organ, aside from the internal control of the Executive, there are no regulations to verify the justification and the procedures to classify any information. Since the Parliament Commission for Secret Funds is not administratively superior to the Executive nor has judicial competences to enforce the Council of Minister to declassify information, the legislative control might be reduced to political explanations and overall statements from CNI and government officials in secret inquiries. To complete the picture, after the regulatory acts of 1995 and 2004 (Laws 11/1995 and 11/2004), the legislative control has been oriented towards the revision of illegal "behavior" of the intelligence service rather than to exercise continuous supervision. Legislative control, therefore, is remarkable reactive in the recent history of this country.

In the case of Brazil, after the ABIN creation in 1999, the lack of clear rules and procedures to establish a legislative control created a political gap that was not filled until the Resolution N.2 of the Brazilian Congress in 2013. By this, the Mixed Commission for the Control of Intelligence Activities (CCAI) should ensure that "such activities are developed in accordance with the Federal Constitution and with the norms of the national legal system, in defense of individual rights and guarantees of the State and society" (art. 2). To achieve this control, the CCAI Commission could access files, areas, and facilities of the SISBIN organizations, regardless of their degree of secrecy (paragraph 4). The CCAI should also examine

and make suggestions to the National Intelligence Policy established by the President of the Republic; making legislative proposals related to intelligence and counterintelligence activities. Furthermore, the CCAI can receive and investigate complaints about violations of fundamental rights presented by any citizen, political party, association, or organization. Notwithstanding, this role has not been activated and is not clear whether this model will be similar to the figure of Ombudsman and Defendant Commission that oversees intelligence services in countries such as Canada and Australia, where complaints are carried by independent commissions or the General Attorney. A sort of Ombudsman figure in the Legislative is inexistent in the case of Spain. Finally, to declassify information, the CCAI must inform the hierarchically superior authority of the SISBIN institutions to decide on the disclosing of the related information. In that sense, unlike Spain, the Parliament Commission in Brazil is able to initiate a process of disclosing information, but the GSI Chief authority that supervises the intelligence system has veto power in this matter.

Both in Spain and Brazil, the Commissions can present amendments to the preliminary report of the annual budget bill, including proposals of additional credits to intelligence and counterintelligence activities. Yet, in Brazil, this ability is incipient and had clashed against other Congress Commissions as seen in the last CCAI sessions. On the other hand, domestic and international links are to be notified to the Commissions. Unlike the Spanish Law 11/2002 that forbids the Parliament to consult information related to the cooperation between Spanish and foreign intelligence services, the Brazilian Resolution of 2013 enables the Congress to request this kind of information. The aim of this point could be related to the national interest of Brazilian representatives to preserve domestic intelligence from the capture by stronger foreign services. Yet, the decision could be a product of a pragmatic approach with no clear motivations. In light of that, the Brazilian Congress Resolution of 2013 is more extensive when it comes to set the Legislative control of the intelligence system than the Spanish norms (Laws 11/1995 and 11/2004). It seems that the Brazilian regulation aimed to fill a gap uncovered during many years in order to "catch up" with the norms from other countries. If the resolution is extensive in some important aspects to enhance a completer and stable control in the hands of the CCAI, in practice, there were no substantial modifications in the role of the Congress to tame the secret services.

For those reasons, some general recommendations can be drawn to improve the legislative control of intelligence. In terms of financial oversight, it should be remembered that the budget cycle of public agencies involves at least four steps: 1) elaboration and presentation; 2) legislative approval; 3) execution; 4) evaluation and control (Wills, 2012, p. 152). Intelligence services are subject to the same cycle, although this usually occurs in parallel and is accessed by a more restricted audience. In general, only the totals of resources allocated to the services are made public. Wills (2012) argues that, in most cases, much more information

could be published without compromising national security and with significant gains in terms of transparency.

At the execution phase, the agency should maintain detailed records of accounting actions and expenditures. The publication of financial reports to internal and external control bodies should be done in two versions: one public, with the suppression of information considered as sensitive, and the other confidential, with restricted access to the controllers of the intelligence services. In order to do so, Wills (2012) also argues that regulations should prohibit services from carrying out financial activities not included in the budget.

In our vision, governments should make public as much information as possible about the intelligence services to the extent that it does not harm public security and national security. Parliaments should lay down rules stating what kind of information (including budgets and reports of the Commissions) should be public or confidential. Brazil has implemented to a certain extent this principle due to the Information Access rules of the country and the mentioned Resolution 2 of the Congress of 2013. Moreover, the Commissions must have the power to audit all aspects of intelligence activity, including special accounts related to confidential or sensitive operations. In that sense, in Spain, the article blocking access to intelligence cooperation with foreign services or groups should be abolished. Scrutiny should take place throughout domestic and international actions, including the budget cycle, starting with the analysis of the confidential sections of the budget proposals, to ex-post review and audit of financial records.

The norms should ensure the external control bodies to access all the information they deem as necessary, whether that information comes from an intelligence body or other public/private entity. There should be sufficient powers to encourage intelligence services to collaborate. Obviously, Parliaments need to adopt measures to protect and safeguard classified knowledge. Besides, the Commissions should incorporate human and technological resources to understand the intelligence activities in order to conduct valid scrutiny. Finally, Parliaments should ensure that the Commissions have sufficient powers to promote the implementation of their recommendations. To achieve this, Parliaments need to create links between internal controls, audit bodies, and Legislative Commissions (including from allied countries) so that results of audits and ex-post recommendations can be implemented in future proposals. Finally, Parliaments Commissions must keep society informed of the control over intelligence services. They should prepare public briefs of their actions and make periodic evaluations of their activities and recommendations. To some extent, this kind of brief was satisfactorily released by the Brazilian Congress.

At this point, the establishment of an independent council comprised of Parliament members, auditors, technicians, and civil society could be an auxiliary

body of external control in the Legislative branch. The members of this independent council would be chosen among citizens with technical knowledge or general expertise regarding the final control of intelligence services. The council could complement the role of the Parliament Commission, as the aim of this model is to enhance a network of accountability that combines political boards (Parliament Commissions) with technical and social expertise (Council) to improve the control and oversight of intelligence.

So far, we have expressed the main aspects of the legislative control over intelligence. Those aspects are summarized in Table 10 below. At this point, what are the overall accountability mechanism and values enhanced by the legislative Commissions in our cases? Both in Spain and Brazil, the legislators were imperfect yet important players to regulate the activities of intelligence and the government by extension. In an overall sense, the intelligence agencies were accountable when regarding the nomination of new Directors; the use of budgets and secret funds (especially in the Spanish case); the formulation of the National Directive of Intelligence (Spain) and the National Intelligence Policy (Brazil); the oversight of intelligence and security cooperation in domestic domains (Spain and Brazil); the oversight of links with foreign services (only in Brazil); and the disclosing of secret information to the public (only in Brazil).

Moreover, the services needed to show accountable actions in case of alleged wrongdoing that most of the times were covered by the media, and obviously after evident failures or scandals, as in the case of terrorist attacks or corruption cases, as in the case of scandals that boosted the creation of norms to control this area during the 90s in Spain. The Commissions demanded accountability through the following mechanisms: By promoting and publishing their legislation and constitutional roles; by controlling the management of budgets and approving specific expenditures every fiscal year; by establishing Public Inquiries; and especially by initiatives or proposals to call intelligence and government members to attend secret meetings according to the norms of the Houses and the Constitution.

Table 10: Accountability in the legislative control.

Accountability dimensions	Cases	
	Spain	Brazil
Who is accountable?	National Intelligence Agency (CNI)	Brazilian Intelligence Agency (ABIN) as coordinator of SISBIN
To whom are they accountable?	- To the Commission for the Control of Reserved Funds (House of Deputies)	- To the Mixed Commission for the Control of Intelligence Activities (CCAI) (House of Deputies and Senate)
About what are the services accountable?	- The nomination of CNI Director - Expenditures and use of secret funds. - Formulation of the National Directive of Intelligence - Overall Plans of Intelligence - Domestic cooperation - Alleged wrongdoing - Explicit failures	- The nomination of GSI Chief and ABIN Director (Senate) - Expenditures and budget. - National Intelligence Policy - "Ombudsman" cases - Domestic cooperation (SISBIN) - International links - Disclosing information - Alleged wrongdoing - Explicit failures
How are they accountable? (measures)	Overseeing the legislation and Constitutional roles, Management of budgets, Establishing Public Inquiries, Establishing Closed Commissions	Overseeing the legislation and Constitutional roles, Management of budgets, Establishing Public Inquiries, Establishing Closed Commissions
Assessing accountability according to its internal principles	Did the accountability action result or promote at least one of the following principles? -Responsibility -Answerability ~~-Transparency~~ ~~-Enforcement (punishment)~~	Did the accountability action result or promote at least one of the following principles? -Responsibility -Answerability ~~-Transparency~~ ~~-Enforcement (punishment)~~

Source: author

According to our methodological operationalization, the performance of public accountability as a connector between authority and sovereignty is a matter of interest. When authority is called to give an account, if that action does not entail more legitimacy, then accountability fails to reach its objective. In that logic, when an authority from intelligence is called to be accountable by soft means, it is possible to speak of accountability by responsibility. When intelligence authorities show responsibility (by fulfilling the duties and measures to them conferred), accountability turns up creating new sources of legitimacy by reconsidering the people that authority is supposed to represent. By demanding a procedural or administrative account, this simpler form of accountability seeks to re-establish the Schumpeterian notion of political representation of citizens and groups of interest in contemporary governments. In this procedural and softer approach, accountability seeks to re-create or maintain the socio-political order: the polity and the consolidation of its administrative processes. In other words, by showing responsibility and representing indirectly the voices of citizens after elections and

formations of governments, this basic form of accountability creates the conditions to perpetuate the very intelligence procedures and institutions as well as the sociopolitical order as a whole.

However, in the legislative control, when an intelligence authority is called to be accountable, especially by the establishment of Commissions, what is primarily demanded is the attachment to the law in order to restrain the actions of the government. In this case, legislative bodies regulate authority by creating rules and overseeing the legal behavior of certain members of the Executive. In doing so, legislators go beyond their mere function of representatives of the people, constraining and demanding respect to constitutional and legal aspects that regulate the socio-political order. Either in open inquiries or in secret meetings with restricted audiences, this kind of accountability resembles the idea of constitutionalism and regulation that characterize contemporary policies. Thus, this form coincides with procedural forms of accountability, such as checks and balances and the division of powers. Accountability here is fostered by mechanisms of formal responsibility but also of political answerability. Hence, accountability in this case not only means that intelligence plans and policies need to have legal grounds. They also need to be politically justified and explained to legislators. Moreover, in the case of alleged wrongdoing or evident failure, the agencies should answer about the circumstances, reasons, and consequences of their actions. Even if the inquiries lack sanction capacities or do not formulate recommendations, the accountability of Parliament Commission serves as constraining tools to shed light upon closed areas from the government. This relates to the notion of horizontal accountability between quasi-equal forms of authorities, between the Executive and the Legislative.

Yet, there are different uses of legitimacy enacted by popular elections or by the formation of governments, and the political powers have different capacities to control each other, especially due to the supremacy of the Executive. The advantage of the Executive was clearly seen in the historical analysis of the legislative Commissions, as several initiatives were ignored by the government, answered in a vague manner during the meetings, or simply were not formulated. Even with the institutionalization of the Commissions, the symbolic value of this kind of control can be expressed in theatrical terms as the inquiries are similar to the performance of protocols. This does not mean that politics are detached from rituals, symbols, and even fictional roles. The exercise of power and its accountability require a form of characterization and performance that permeates every social domain. However, the efficiency of accountability by the Legislative power is poorly circumscribed to the promotion of responsibility and answerability principles, as attested in this section. In that sense, more principles and roles need to be fostered to increase the quality of accountability, such as more transparency and enforcement. Thus, in the next section, we turn to the judicial role of Courts as mechanisms to control intelligence.

3.6. Judicial control

Considering the judicial control of intelligence agencies, the Courts face again the old dilemma of disclosing official secrets. In the theoretical discussion, we mentioned the existence of state secrets illustrated in various writings of the sixteenth and seventeenth centuries (the *arcana imperii*) and the connection to the reason of State explored by Machiavelli and Hobbes. In light of this, the poles of confrontation are, on the one hand, the sovereign power from the Executive (and the ways of maintaining its power) and, on the other, Law interpretation from the Judicial control, as a technique for limiting the decisions of the former.

Hence, in this section, we will illustrate the legal dilemmas to access the information of official secrets by the judicial power. Then, we will assess the judicial role to control intelligence in both case studies.

From the judicial point, Spain is deemed as a democratic state of rights. For example, several principles are guaranteed in the Constitution to oversee the actions of the state. For example, "the judicial proceedings shall be public […] and predominantly oral, especially in criminal sentences that shall always be reasoned and pronounced in a public audience" (Article 120, Spanish Constitution, CE). Moreover, the Constitution expresses publicity and transparency as principles to be projected on the three branches of the state, being a structural demand to guarantee the exercise of rights and freedoms of citizens. However, there are also constitutional foundations that allow the state to evade publicity and transparency in certain matters that, by their content and characteristics, could be declared reserved or secret in their integrity. The Spanish administration may deny access in the following cases:

a) If documents contain data referring to the privacy of persons. In this case, if the documents include specific names and personal information, only the referred persons or their representatives are able to access or request the information.

b) If documents contain information on acts of the Central and Autonomous Governments or matters related to national defense or state security;

c) When documents might endanger the protection of rights and freedoms of third parties in the case of the investigation of crimes; and

d) In the case of documents that refer to administrative actions derived from the monetary policy.

In the second point (b), which is our focus now, the Spanish Constitution of 1978 grants exclusive competence to the state on matters of "defense" and "national security". This decision is based on the sovereign capacity to decree the

reason d'état and the exceptional powers to preserve the socio-political order, as discussed in the theoretical framework (Chapter 1). In the same logic, to exercise these powers, the Spanish state can deploy Armed Forces and Security Forces. These actors should "guarantee the sovereignty and independence of Spain, defend its territorial integrity and the constitutional order" (Article 8.1, C.E.). Thus, "security and defense of the state" are presented as the paradigmatic domain that is susceptible to being subtracted from the general principle of publicity. Therefore, the records of those matters in public registers and archives are an exception (Article 105, C.E.). This prerogative is not unique to the Executive. The Parliament may also hold and deliberate decisions in secret sessions provided that they follow the will of the absolute majority of members and the regulations of the Legislative Houses (Article 80, C.E.). In addition, the Judicial Power, through the provisions introduced in the procedural order, may restrict the publicity of certain aspects and processes as in the case of criminal and enforcement investigations (Article 120.1, C.E.).

However, there are also specific legal mechanisms that establish secrecy for national security and intelligence. This is the case of the so-called Law of Official Secrets.

Law 9/1968 of Official Secrets (LSO), modified by Law 48/1978, establishes the general exceptions to the principle of public access. In that sense, Articles 2 expresses that "classified matters are the issues, acts, documents, information, data and objects that could damage the security and defense of the state if disclosed by unauthorized persons". Moreover, Article 13 declares that classified materials cannot be communicated, disseminated, and published outside the limits established by LSO. "Failure to comply with this limitation will be sanctioned as a very serious offense in accordance with the Criminal code" (Article 13, Law 9/1968).

According to the LSO, both the Legislative and the Executive can declare secrecy of information. For example, the Executive can establish the mentioned Reserved Credits or Funds for security, foreign affairs, and defense. That is, the limitation of the constitutional publicity principles can be implemented through a single act of "classification" by the government. Ruiz Miguel (2005) affirms that classifying is a "political" and "administrative" procedure. According to the LSO, only the Council of Ministers and/or the Chief State of the Armed Forces have the capacity to classify and disclose any official information. In this action, the formalities and the motivations for classifying something are taken behind closed doors. Thus, LSO highlights a political and tautological logic: the "sovereign" classifies something because something needs to be classified (to the eyes of the sovereign).

Classified information in Spain has two categories: “secret” and “reserved”. The first category means that the matter requires the highest degree of protection due to its exceptional importance. Besides, disclosure is not authorized as it could compromise the fundamental interests of the state in matters related to the national defense, foreign peace, and constitutional order. Meanwhile, the “reserved” category is related to a degree of risk, as its disclosure could result in lower damage to the mentioned fundamental interests. Ruiz Miguel affirms that the only difference is that the category of "reserved" applies to matters of “minor importance”. The legal consequence of that distinction entails practical effects, as in the case of the regulation to access intelligence information by the Parliament (see the previous section).

Resolution of the Council of Ministers on November 28, 1986, affirms that the category of “secret” relates to matters such as the procedures, techniques, and sources of the intelligence services. Moreover, “secret” matters refer to the National Defense Directive, the information, analysis or evaluation of current or potential threats to peace and security in Spain, the General Plan of National Defense, keys and cryptographic code material, reports and statistical data on military movements and forces, maneuvers of battleships or military aircraft, etc. In the same Resolution, the category of “reserved” was given to the following subjects: the destination of the personnel of special character, the security plans of public institutions and bodies, units, centers or agencies of the Armed Forces, and centers for the production of war material.

The consequences of the classification of any information are various. Firstly, it restricts the publicity of certain issues, prohibiting access, and limiting the circulation of unauthorized persons in specific places or zones. Secondly, it obliges any person that receives any “classified matter” to keep the secrecy and to contact civil or military authorities for its custody. However, disobedience to this obligation was not sanctioned, as attested in cases such as the “CESID papers”, in which classified materials reached unauthorized persons (bankers or journalists) who in turn did not return the information to public authorities. Thirdly, classifying requires a series of security measures such as custody, transfer, transmission, registration, inventory, examination, and destruction of classified material. Notwithstanding, disclosing secrets and reserved information constitute a crime as established by the LSO, but this obligation is projected especially to public officials and personnel that work in the administration.

On the other hand, the legal system protects the activity of intelligence by means of “professional secret”, which consists in allowing one exception in the duty to collaborate with justice. Thus, when the courts demand the participation of intelligence professionals, they cannot be compelled to “violate the secrecy of the professional code, or to give information without the formal authorization of their superiors” (art. 417.2 Law of Criminal Procedures). Finally, if the media releases

information related to official secrets from oral sources, third parties, or because the document was physically accessed, the responsibility falls directly on the person who violated the LSO. In case there is a physical or analogic transference of documents, the Courts can prosecute both the discloser and the publisher of the information (González, 2019).

Use of official secrets in other countries

In the Anglo Saxon world, for example, the access to official secrets and activities of information services escapes from citizen control, but the legal systems maintain the right to information as the backbone of the democratic order. In the United States of America, the *Freedom of Information Act* guarantees the right to information since 1966. The Act guarantees the right to request information and obliges the government to disclose it respecting the limits of privacy and national security. Although the Freedom of Information Act entered into force in 1967, it was not applied to intelligence files until 1975. The procedure is relatively simple: when a petition is received by enforcement authorities, this one is copied and examined by an analyst who determines if there are parts of the file that deserve to be declassified, justifying this decision. Thus, the provided copy could be censored in some parts by the "pen and marker method". Through the *Freedom of Information Act*, citizens have access to any classified information, as long as they do not affect people's privacy and national security. In this case, a temporal declassification category applies, so the citizen can know the actions of their security and intelligence services even decades later. This process exposed, for example, historical events such as the Watergate political espionage, in which Richard Nixon used the intelligence services for partisan interests and to surveille the opposition. The same method also revealed the systematic use of torture by the CIA in the context of the War on Terror in Guantanamo since 2001.

In the United Kingdom, the Public Records Act of 1958 regulates the disclosure of information. Since 1967, the Act was updated many times to introduce minor changes related to the list of organizations that integrate this issue. In 2000, the law was modified allowing reports from the intelligence sections to be consulted via the Office of Public Information. Although the third section of the Act determines that those files are not open to the public, different departments can release classified materials, without depending on the request of a citizen, but on the initiative of each Ministry. Furthermore, the Act establishes that the secrecy of documents lasts up to 30 years. Each year, several documents are declassified on January 1, 30 years after the last date of their creation. The annual disclosing of public reports is known as "new year's openings". Some documents might be classified for longer periods as in the case of "extended closures" of documents that have their secrecy renewed for 50 or 75 years. Finally, the Lord Chancellor or Lord Keeper that oversees the policies for official secrets can disclose documents at any time but reporting this action to the Parliament.

Considering the Spanish case, the regulation on access to official archives varies according to the historical period. According to the LSO of 1968, classified materials do not receive an expiration date. Unlike regulation from other countries, the Spanish official secrets lack temporal limits or an automatic process of disclosing. This has caused many critiques from researchers and historians who study the Late Franco Era and the so-called Spanish Transition. Constitutional and criminal law scholars (González Cussac, Hinojar, & Hernández, 2012) argue that the purpose of keeping recent material as secret has no rational-legal justification.

In the same logic, José Antonio Sainz Varela, director of the Provincial Historical Archive of Álava, argues that the category of "secret" has been overused by governments beyond the protection of issues related to "trade, diplomacy, industry, and national defense" (Sainz Varela, 2018, p. 110). Therefore, the LSO inhibits transparency and deeper historical opportunities to understand the last years of the Franco regime, the Transition, and the coup d'état of 23-F. Moreover, the rules shield the government and the Courts against petitions from victims to clarify the official violence executed during the Transition, as well as the examination of the roles regarding the information and intelligence services during the recent times.

In the last years, the former Defense Minister Carmen Chacón attempt to disclose thousands of documents was blocked by her successor, Pedro Morenés. In addition to the limits imposed by the LSO, the Spanish Historical Heritage Act of June 1985 also establishes that "documents containing personal data; and any other procedures that affect the safety of people, their honor, the privacy of their families and their image, shall not be publicly consulted without the express consent of those affected" (Article 57.1.C). According to this Act, there are two temporal lines to declassify information: twenty-five years after the death of the affected person (in case the person related to the documents is known), or fifty years after the creation of the documents. In addition, regulations for the protection of personal data also establish limits to access documents and files (see Chapter 4).

Furthermore, many police documents related to the political transition have not been transferred to historical archives in order to be stored and analyzed. Many documents were destroyed, especially in the case of the archives related to the official party of the Franco regime, FET, and the National Movement, JONS. This destruction also affected information stored by the Social-Political Brigade and by the Civil Guard, including the files related to their information services. Finally, when the documents are stored in public archives, access to those files must be conducted through the criteria established by the mentioned regulations (LSO and Historical Heritage Act).

Regarding the judicial control of official secrets, until the reform of the Center of National Intelligence (CNI), in 2002, the position of the Supreme Court and Constitutional Court to support a legitimate intervention on communication and life of citizens was based on "public safety" principles. That is, to the Courts, the Security Forces embodied limits to political and civilian liberties as they were entrusted with "the maintenance of public safety" (Article 1.4 LOFCS). From this perspective, only the "Information Headquarters of the Civil Guard" and the "General Information Office of the National Police" were able to request authorization for such interventions. The CESID and the military information services were deprived of this possibility because they were not inserted in the

paradigm of “public safety” in Spain. Since the CESID was not a "police" with the capacity to initiate judicial investigations, this produced a gray legal zone where intelligence activities were executed with no legal warrants. When illegal interventions happened, they were simply ignored as no legal and judicial control existed before the creation of the CNI. Before 2002, the CESID usually gathered information from not open sources and by using covert actions. This type of information could have been obtained by unconventional methods ignoring the legal system. The jurisdiction of that time understood that the CESID internal regulations entrusted agents to carry out actions that “required special means, procedures or techniques” (Ruiz Miguel, 2005, p. 135). That is, the Center had leeway to collect information and deploy agents –including surveillance methods- by extraordinary means that were verified only by internal controls. In the meantime, the CESID developed techniques of interception such as technological-cryptographic research and training of human intelligence (HUMINT) with no substantial external controls.

The lack of external controls in intelligence was an object of attention during the 1990s. In terms of Legislative control, we mentioned that the Parliament started to oversee the use of “Reserved Credits” protected by the LSO. The control of those credits caused a series of debates and discussions. As Bueso (1997) mentions, the use and misuse of Reserved Credits caused turmoil at the beginning of the VI Legislature (1993-1996). In those years, the “sacred sphere” of state secrets was shaken in two directions: a) the first one was related to a sector of the House of Deputies (especially directed by groups such as *Partido Popular* and *Izquierda Unida*) who were interested in reviewing the scope and limits of the government, and b) The second direction related to the access of official secrets by the Courts and magistrates. The last direction raised the possibility to investigate and prosecute crimes stemmed from cases such as *Roldán*, *Rubio,* and *Banesto*. These cases emerged when the former Director of the Civil Guard, Luis Roldan, sued the Defense Minister García Vargas and the Vice President of the Government Narcís Serra after they used reserved credits to pay international private detectives specialized in economic intelligence (the Kroll agency) to investigate the activities of the former president of Banesto Bank, Mario Conde. The Supreme Court accepted Roldan’s accusation but, according to the court, the use of reserved credits for this kind of investigation did not imply in “incorrect use” of funds. The Court understood that the banker might have committed crimes provoking serious risks to the national financial system, justifying, thus, the relevant public interest and the access to reserved funds to collect evidence (Ruiz Miguel, 2005).

After those cases, the judicial control of classified documents was raised for the first time when the Court of Instruction 5 of the *Audiencia Nacional* (a National Court) issued the Ministry of Defense to concede secret documents on October 11, 1995. As the Ministry of Defense refused the petition, the judge filed a complaint accusing the Ministry of causing conflicts of jurisdiction. The Constitutional Court

rejected the accusation arguing that, when considering information classified as secret by the Council of Ministers and by criminal instructions, these matters were not objects to judicial control (Ruiz Miguel, 2005).

One year later, the courts clashed against the government again modifying the doctrine with a new solution: By the examination of official documents *in camera* (behind closed doors). This time, to dodge refusal by the government, the courts claimed the right to obtain effective protection and justice in every judicial and courts instruction (Article 24.1, CE), as well as the right to use relevant evidences of proof by the defense and defendant (Article 24.2, EC). The claims were solved by the Supreme Court that agreed on the disclosing of the secret documents by the government in 1996. The long process to disclose information is related to the Spanish constitutional framework, which follows the European-continental model in which the courts have their powers assessed by rules (they can only act within the strict interpretation of the norms). This is slightly different, for example, to the judicial framework of the Anglo-Saxon model, in which the courts have their capacity of sanction and veto power enacted by legal rules and by customary laws.

As mentioned, intelligence services do not investigate crimes, nor seek to obtain evidence of illicit behavior for prosecution purposes. The Spanish legal system attributes these functions to the State Security Forces and Police Corps (Police agencies and Law Enforcement institutions). We also mentioned that the National Intelligence Center (CNI) is the public organization responsible for providing the President of the Government the information and analysis to prevent any danger, threat or aggression against the independence or territorial integrity of Spain, to the national interests and the stability of the Rule of Law (Law 11/2002). To accomplish those missions, Article 1, Law 11/2002, attributes specific functions to the intelligence service: "To obtain, evaluate and interpret information and disseminate the necessary intelligence to protect and promote the political, economic, industrial, commercial, and strategic interests of Spain."

From this point of view, the principle of circumstantial intervention would not apply to the typical actions of intelligence services. The constitutional principle of indicial intervention refers to the investigative capacity of public authorities to prosecute crimes. However, several questions emerge when intelligence services execute their missions. For example, it is necessary to balance the restriction of rights and the constitutional goals of intelligence services (defined by Law 11/2002). Moreover, intelligence interventions of constitutional principles (such as publicity, dignity, non-interference of communication, and so on) need restrictions. Intelligence should take into account that there are no other less aggressive means or methods to achieve the specific goals. Finally, when intelligence interferes with those principles, there must be proportionality in this action, weighing the seriousness of the intervention and the reasons that justify

them. In simple terms, the perception of threats and the restriction of rights must be balanced in every situation (Morales, 1999).

Therefore, the CNI interventions must follow the principle of proportionality in temporal and spatial aspects. This principle demands a basic level of guarantee: a law that becomes a guarantee of other rights. That is, the rule must be clear and universal to regulate those cases in which citizens' rights may be limited. For example, one of the rights that could be restricted by intelligence is obvious: the right to life. The first title of the Spanish Constitution, on Fundamental rights and public freedoms, begins precisely with the recognition of the right to life as a core principle. Without it, "the remaining rights would have no possible existence" (STC 53/1985). In addition, Article 15 from the Spanish Constitution includes the right to physical integrity and moral integrity, prohibiting the death penalty, torture, and inhuman or degrading treatment. The performance of intelligence services finds a clear limit in this right. In turn, moral integrity entails a plurality of other rights: the right to physical integrity, right to physical and mental health, right to physical and mental well-being, and so on. From a judicial perspective, moral integrity has been defined as "the right to preserve the individual autonomy, prohibiting treatments that nullify, modify or injure individual will, ideas, thoughts, and feelings […]. These rights are expressions of human dignity; the use of methods or procedures to alter them, including torture, constitute inhuman or degrading treatment" (Díaz Pita, 1997, p. 53).

The judicial interpretation above stems from the jurisprudence established by the European Court of Human Rights. To this Court, torture, inhuman treatment, and degrading treatment are located on a scale of intensity imposed on some person. In that sense, the "minor" level regards degrading treatment, as it could be considered as the act that provokes fear, anguish, and inferiority to humiliate a victim, degrading and, eventually, breaking his/her physical or moral resistance (Rodríguez, 2014). However, in practice, it is difficult to assess a priori those categories insofar as courts investigate the magnitude and level of damage inflicted in a posteriori form, only during trials. Yet, the judicial principles embodied by the European Court and the Constitutional Court serve to protect core rights related to individual autonomy, a matter of interest to this study.

In Spain, intelligence might also affect other rights such as publicity and freedom of information, as those rights are connected with the classification of matters related to defense and national security. Access to this information is limited in every legal system (we have seen that disclose this information is even difficult to Control Commissions in the Parliament). Nonetheless, information about intelligence and intelligence products are not absolute and cannot be placed out of controls. The absoluteness of intelligence, and security and national defense, would go against the most elementary democratic principle of accountability between public powers. That is, intelligence indeed could interfere and limit

freedom of expression and publicity, but, in doing so, it must proclaim the ways and criteria to conduct this interference. Intelligence cannot be a *carte blanche* to override fundamental rights. Intelligence should be understood as an exceptional measure to suspend those rights in order to protect them. With this, the dilemma between intelligence (and security by extension) against fundamental rights (and democracy by extension) could be solved as they are not antagonist sides of a clash. Rather, the former is operationalized to simultaneously suspend and preserve the latter. Suspending freedom of information, in this case, constitutes a necessary measure to sustain a society of rights and plural information. In short, the suspension is contingent and limited by the own teleological principle of sustaining and enabling the proliferation of a space in which civil rights are exercised despite the threats embodied by external circumstances or by the rules that are operationalized to protect them. Thus, it is important to consider and scrutinize governments when they refuse to disclose documents even at the request of the Supreme Court, producing, then, restrictions to the right of freedom information. In that sense, the role to disclose information can be expanded to other actors in the legislative and judicial branches in order to promote more external control. Currently, the LSO only authorizes the Government and the Board of Chiefs of Staff of the Armed Forces to classify and disclose any information (whose knowledge by unauthorized persons may damage or endanger the security and defense of the state).

To expand that role, we mentioned the importance of parliamentary regulations to improve the external accountability of intelligence. In terms of judicial control, the Organic Law 2/2002 enables the Prior Judicial Control of the CNI and complements Law 11/2002, of May 7, which regulates the National Intelligence Center. Law 2/2002 modifies the Organic Law of the Judiciary, defining a judicial control to the activities of the Center that affect fundamental rights recognized in articles 18.2 and 3 of the Spanish Constitution. Article 18 of the Spanish Constitution requires judicial authorization for activities that affect the inviolability of the home and the secrecy of communications. In turn, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms requires that those interferences need to be recognized and regulated by law. Thus, the articles recognize the intelligence ability to interfere with the fundamental rights of citizens, regulating this interference and covering a gray zone that was untouched during the CESID years.

The prior judicial control of the CNI (Law 2/2002) refers to the rights contained in article 18.2 and 3. Yet, no mention is made to article 18.1, which includes the right to honor, personal and family privacy, and individual image, or to article 18.4, which limits the use of information technology to guarantee the honor of persons and the family/personal privacy of citizens. Furthermore, neither the CNI Regulatory Law nor the Organic Law of Judicial Control mentions rights related to personal data, as this information could be affected by the performance

of intelligence services. Therefore, the prior judicial control is limited, especially if we consider that the CNI activity of "espionage" is similar to article 7 of the Organic Law 1/1982, of May 5, which describes different forms to collect, track and capture personal information that affects and interfere with personal communications.

Naturally, there is no mention of the term "espionage" in the CNI regulation and we do not mistake the CNI activities with this word. The CNI regulatory laws mention that the Center obtain, evaluate and interpret information and disseminate the intelligence necessary to protect and promote political, economic, industrial, strategic and commercial interests of Spain, being able to act inside or outside the national territory (art. 1, Law 11/2002). CNI members are not considered agents of policing enforcement. The service also cannot detain, interrogate, or submit a person to conditions or procedures that involve physical or mental pain. If the intelligence services discover a crime during the exercise of their activities, they should activate other security agencies that cooperate with Justice. In turn, the CNI obtains information and develops intelligence about matters that affect national security or the state, helping the government to take decisions by procedures that are reserved or secret. Yet, these lines are implicitly compatible with espionage activities deployed without the consent of targets or people. History has shown that intelligence services can spy even when the regulatory norms say the contrary or omit this issue. For this reason, the regulatory norms of the CNI, including the Law of Judicial Control, should have included the intromissions in personal privacy as rights that need prior judicial authorization, preserving also the honor of persons, and the family/personal privacy of citizens.

Intelligence regulatory norms consider the inviolability of home and communications as concepts in which a certain person maintains a private life without interference from other people, but not from the state. Privacy can indeed be defined as the right to be left alone. However, informational monitoring and technological tools allow the "unlimited" gathering of information that can be stored or processed in many ways. This is not only a matter of privacy, it is no longer about a right to deny information or hide something. As discussed in Chapter 1, privacy is also a right to have information, to preserve identity, to consent, to control, and to rectify data monitoring concerning personal information. The right to keep control of personal data redirect us to Article 18.4 from the Constitution that entails the right to information and self-determination. This article empowers the individual to decide, about the delivery and use of personal data, prohibiting storing this data for undetermined purposes. Thus, it is pernicious that personal data scopes are not even mentioned in intelligence norms. Law 2/2002 does not include personal data within its scope of application, leaving the judicial control established in the actions of the CNI out of the fourth section of Article 18 of the Spanish Constitution. Notwithstanding, the reversal is also true. Personal Data regulations also exclude intelligence from their scopes and

purposes. “The provisions of paragraphs 1 and 2 of article 5 will not apply to the collection of data when the information the affected when it affects the National Defense, public security or the prosecution of criminal offenses” (Article 24 of the Law 5/1992 of personal data protection). Since intelligence and rights related to intimacy, privacy, and personal data are very close, the exclusion of the Organic Law of prior Judicial Control of those matters is paradigmatic.

For intelligence purposes, it is also true that public events in open places are not part of the sphere of privacy. In physical or cybernetic spaces, it is possible to think about cases in which a person allows an audience to know her habits and customs in exchange for privacy. Yet, if someone needs to collect more information about this person, for example, by installing a hidden micro-camera inside a vehicle, this action crosses the line of public spaces of information and affects the right to privacy (Article 18.1 of the Spanish Constitution), although it does not entail a violation of domicile or property (Article 18.2).[56] Let us consider other examples. The use of computer data to cross variables and databases might allow knowing private and constitutionally protected aspects. Allowed without limitation, the repeated track and monitoring by computer algorithms could entail knowing aspects of privacy and making us all suspects in the eyes of intelligence. The actions of the CNI, in this scope, are justified by the criterion of “the security of the State” and the “fulfillment of its functions”. However, this kind of automatic and mass surveillance is not an object for judicial control. The proportionality of intelligence actions in these cases is inexistent. In the case of Spain, the balance and protection of fundamental rights, even in these cases, can only be balanced in the performance of the CNI in each concrete situation, as determined by Law 2/2002. Yet, there is no way to know if the magistrate of Justice has the jurisdiction to oversee and whether is capable to balance the impact of automatic and electronic surveillance of the Spanish intelligence in the domestic territory. In the case of electronic surveillance, it seems that the control depends on internal audits, technological development, the security of information standards, and cooperation between security agencies, rather than judicial and legal controls, especially in the realm of intelligence. In short, there is a differentiation between targeted surveillance (that interfere with rights of specific persons) and mass surveillance (that interfere with the rights of entire populations) in terms of

[56] On the work of monitoring and observation of suspicious persons, the Supreme Court has said the following: "through the visual and direct perception of the actions performed on public streets or in any other open space (...) image capture is authorized by law in the course of a criminal investigation provided that it is limited to recording what happens in public spaces outside the inviolable precinct where the exercise of privacy takes place. Therefore, when the location of filming or listening devices invades the restricted space reserved for the privacy of individuals, it can only be conducted by virtue of an injunction that constitutes an enabling instrument for interference with a fundamental right. These interventions would not be authorized without the appropriate judicial control, including the means of capturing image or sound inside the home, and other technical forms of recording devices, even when the capture takes place out from the domiciliary precinct" (Supreme Court-Room 2- Decision of May 6, 1993).

geographical scale and constitutional impacts. Yet, both of them need to be contemplated in the judicial controls of intelligence. We cannot assure the CNI capacity to conduct mass surveillance (in terms of legality, it is a practice that could not be conducted by the service). However, as technological developments facilitate and increase this kind of surveillance, the constitutional and judicial norms should contemplate that possibility (Barrilao, 2019). Otherwise, this gap would open a tremendous gray zone in which surveillance mechanisms are exercised without sufficient judicial grants.

In that sense, we remind that the unlawful (not legal existence) and illegal (acting against the law) interference of private communication by intelligence was a paradigmatic case that entailed the reform of the Spanish service. After the leaks of the SECID papers during the 90s, the legislation of the CNI and its judicial control was justified to protect a fundamental right. National security cannot justify systematic conduct that violates fundamental rights without external controls. Judicial doctrines, such as the No. 43 Order of the Court of Instruction of Madrid on February 6, 1996, which argued that random and indiscriminate eavesdropping by intelligence services were expected since they can execute certain activities without establishing the means to be used for their achievement, should no longer be tolerated.

At the end of the 1990s, the European and Spanish judicial doctrine learned from important cases of illegal or unauthorized wiretappings that interfered with personal communications. One lesson is related to the Traube case that led to the reform of the German Constitution in 1998. After this case, the European doctrine supported the idea that the prosecution of suspects of serious crimes could be accomplished by judicial authorization, and by the technical means necessary to clarify the circumstances of the investigation. Thus, the first step to a proportional enforcement action is based on suspicion as a characteristic taken from granted to activate judicial investigation. Yet, this "pre-accusatory" characteristic should be submitted to a deadline that enables the investigation by the signature of a Court integrated by three judges (paragraph 3, Article 13, German Criminal Code). In order to manage urgent situations of danger to public safety, especially in cases of general risks for the lives of people, technical means such as home surveillance can be placed only by judicial authorization. In case the authorization cannot be provided in advance, and because of the imminent threat, this must be obtained as soon as possible. If the technical means are exclusively oriented to the protection of the persons participating in a security intervention, the actions should also be conducted by legal warrants. By the German Criminal Code, only evidence and information legally collected are valid to prosecute or to guarantee public safety. The Federal Government report annually to the Bundestag on the placement and number of technical means carried out based on those interventions. Thus, the government reports a basic form of answerability even if the acts and contents of the investigations are restricted from the public.

In light of the above, the German doctrine influenced the principles of the Spanish prior judicial control of the CNI. The Spanish legislation understood the intervention of communications as a matter that might help to clarify actions that endanger the national security and the purposes defended by the intelligence service. In that sense, the intervention of communications can only be adopted within a process that guarantees the adequate control of the measure by a judge, whereas the targeted person ignores the intervention. These judicial criteria were reconsidered after the CESID Papers and wiretapping cases mentioned above. In these cases, CESID technical teams wiretapped lines and recorded conversations maintained by private citizens. Even the information that was of no interest from the operational point of view was simply stored and preserved. After these cases, no rules can allow the intelligence service the power to intercept citizens' communications if there are no indications that those are related to their missions. Moreover, to legal effects, those interceptions are valid only if they are conducted with judicial authorization and judicial control during the monitoring. Otherwise, intelligence activities would be a mere tool for "the reason of State" that is incompatible with the Rule of law (Bueso, 1997; Barrilao, 2019).

In that sense, the Director of the CNI must request authorization from the Magistrate Judge to deploy measures that affect the inviolability of the home and the inviolability of communications, provided that such measures are necessary for the fulfillment of the Center's functions. Law 2/2002, paragraph 2 demands that the written request must include the specification of the measures, the facts on which the request is supported, and the purposes that motivate the intelligence action. Besides, the Law demands the reasons that recommend the adoption of the interference, the identification of the person(s) affected, if they are known, and the designation of the place where they are to be practiced. Besides, it demands the duration of the requested measures, which may not exceed 24 hours in the case of interference with the inviolability of the home and three months for the interception of mail, telegraph, telephone, and other communications. The Magistrate Judge can renew both terms of intervention for equal periods. Finally, the Magistrate Judge must grant or deny the authorization weighing the circumstances that justify the suspension of the fundamental right, the proportionality of the measure, and other ways to fulfill CNI functions that are less intrusive. In short, the Magistrate needs to assess the indications that national interests are in danger and the proportionality of the intervention.

The motivations and justifications that the CNI should demonstrate before a Magistrate Judge are a leap towards the improvement of judicial accountability. Yet, as Pérez-Villalobos (2002) suggests, judicial control is not perfect and can be improved, especially if we consider the following points:

1. Intelligence services have an important constitutional function (Article 1.1 CE) and are regulated by external controls (stemmed from Laws approved by The

Parliament and the Senate). In that sense, regulating the procedures and guarantees affected by intelligence was really essential, even when intelligence services are not essentially espionage services. However, the Prior Judicial Control seems more oriented to provide a veil of judicial appearance to the activities carried out by the CNI, rather than to consolidate the content of what should be an authentic judicial control (Pérez-Villalobos, 2002). At this moment, we cannot prove or discredit this point.

2. The number of persons who "watch the watchers" is another important point. In that sense, the creation of a trained body of at least three Magistrates would be a more efficient way to control the CNI activities. This control, based on the European jurisprudence, would be deepened and strengthen if more Magistrates oversee the measures requested by intelligence. In 2001, before the Law 2/2002 was enforced, criticism arises due to the unipersonal model of judicial control in Spain. According to Pérez-Villalobos (2002), the competence of the second Chamber in the plenary session of the Judicial Power debated modifications in this point, but the text proposal was sent to the Parliament without modifications and preserved only one judge and a substitute (Official Bulletin of the Cortes Generales, of December 20, 2001, No. 132).

3. The items 3 and 4 of Law 2/2002 mentions that "The General Council board shall report, in all cases, the appointments of the plenary's jurisdiction, except in the case of the appointment of the Supreme Court Judge provided for the article 127.4", that is, except for the Magistrate who controls the intelligence service. For Pérez-Villalobos (2002), this exception does not favor transparency in the appointment of the Magistrate who specializes in the control of intelligence services. In other words, the exception to indicate a judge on this issue gives the impression that the CNI owns a favorite magistrate, either by prior selection or by indicating one Magistrate "a la carte". In our vision, the election of this Magistrate should avoid special appointments or exceptions, even this person oversees exceptional tasks for the national security and safety of the state.

4. Law 2/2002 specifies that the authorization request must contain the fundamental elements that interfere with fundamental principles of Article 18 of the Spanish Constitution. The positive part is that the judge must receive important information from intelligence, such as the justification of the requested interference, the facts on which the request is based, and the duration. Yet, this content, even if necessary, is not enough because the judge would need to have a more concrete knowledge as the text of the Law allows the Director of the CNI to provide only basic information to the judge. This means that the Magistrate will not be able to adequately weigh the proportionality, even though the law says that "the Magistrate will employ a reasoned resolution within seventy-two hours

conceding the approval or disapproval of that measure". The Law is also not clear in cases in which the Magistrate reject proposals that are not fully justified.[57]

5. On the other hand, the duration of the requested measures may not exceed 24 hours in the case of the inviolability of the home and three months for the intervention or interception of postal, telegraphic, telephonic, or any other type of electronic communication. Both terms can be extended by continuous periods, according to the section 2.d of the Law 2/2002. However, the regulation does not establish how many extensions can be given by the Magistrate, or what is necessary to concede another time extension. That is, in case the intelligence service does not find what is looking for after the first interception, the jurisdiction makes no suggestions in what the Magistrate should do or expect to authorize another time extension.

6. Section 4 of Law 2/2002 attributes to the Director of the National Intelligence Center the responsibility to erase the information that is not related to the scope and purposes authorized by the Magistrate. However, the Magistrate does not supervise the deletion and he/she cannot even verify whether the authorization has been respected and followed. For Pérez-Villalobos (2002), this makes the control become a purely formal act, and not a real and effective judicial control. Finally, the possibility of a legal reaction of citizens to illegitimate actions of the National Intelligence Center is not even considered. At this point, we must remember that the Constitutional Court 49/1999 recognized the right of one person, whose fundamental rights and freedoms were interfered, to know the judicial actions and react when the measures are over. Therefore, it seems that it is an inalienable constitutional requirement that the actions must be reported when the situation of danger to the security of the state disappears, as this idea is the main reason to adopt secrecy. There is no use in enacting a system of protection of rights if the subjects have no remote chance in knowing, even in a posteriori form, the interferences they have been subjected to. Having no chance to react and support individual rights, especially in case of wrongdoings or mistakes by a public institution, is not admissible. In that sense, Díaz-Fernández (2005) has even proposed the creation of Ombudsman figures with capacity do exercise internal audits on intelligence services and support the defense of rights and to complement the judicial power, especially in the case of false positive targets and potential victims of intelligence. Finally, as the judicial control of the CNI is exercised in a priori terms, no judicial or administrative institution, aside of the Parliament (which only oversees intelligence by the rules of the Commission for

[57] An amendment submitted by the Izquierda Unida Parliamentary Group sought the inclusion of a paragraph with the following text: "The Magistrate will take into consideration in his decision to authorize or disallow the actions of the CNI the necessary balance between the values of security and freedom in a State by social and democratic law, weighing the risks to the general interests of the Spanish State and the dangers to the fundamental rights of citizens" (Official Bulletin of the Cortes Generales, February 7th, 2002, Series A. No. 58-5).

the Control of Reserved Funds) controls the legality and procedures after the Magistrate authorizes the CNI operations. After the Prior Judicial Control, intelligence activities enter in another gray zone, alongside the mentioned automatic and electronic mass surveillance. Naturally, those activities are conducted and protected by the LSO of official secrets. Yet, the secrecy of the state should not mean permanent or eternal secrecy for the public or something outside the range of justice.

*

Regarding the Brazilian case, the power to classify official information is also part of the *arcana imperii*, the authority that sustains the sovereignty of the state. As mentioned in Chapter 1, every form of power contains a certain level of secrecy. At the imminence of becoming total transparent, power becomes something else, a theatrical stage where political actors perform their playing. However, there is also a demand for transparency to illuminate the acts of government. It is important to know the acts of the state insofar as they show "how citizens are governed". For Bobbio (1989), the idea behind *custodiet ipsos custodes* (who watches the watchers?) is a fundamental question. For him, if we cannot find an adequate answer to this question, democracy (and legitimacy) is lost. "More than an unfulfilled promise, [controlling the watchers] does not entail the maximum control of power in the hands of citizens. Rather, it restrains the powerful ones to control the citizens" (Bobbio, 1989, p. 158).

In that sense, intelligence supervision and control emerged from the lack of tools to oversee secret services. In many countries, the greatest incentive for the change in accountability was sparkled by scandals involving abuses of power and violations of individual rights by intelligence agencies. For Gill (2003), those changes are attested in the United States Congress inquiry commission (1975-76) (Senator Church and Deputy Pike cases), the McDonald inquiry of the Canadian Security and Information Service (1977/1981) and Hope's judicial inquiry of the Australian Security Intelligence Organization (1976-1977, 1984/1985).

In countries of transition that experienced authoritarian regimes, such as Brazil, Cawthra & Luckham (2003) express different steps for reforming intelligence services. The first step is reforming or dismissing officials and personnel engaged in repressive activities while clear rules should be established for this activity. The second step consists of Congress or Legislative control, which basically oversees the intelligence budget and plans. Yet, to those authors, the most important step is the Judiciary power to control routines and operational matters in which the intelligence agencies suspend citizens' rights, such as privacy. In the Spanish case, we expressed the problems to establish and implement ex-post judicial control. Those scholars have also mentioned the need to include an

institutional channel to receive complaints from individuals for alleged damages caused by intelligence activity, something that still does not exist in Spain.

Considering the potential power of intelligence to alter the rights of citizens, Brazil also protects privacy as one fundamental right. Article 5 of the Brazilian Constitution of 1988 mentions that privacy is protected in "mailing and electronic communications of national and foreign citizens." Yet, the exception to this protection can be established by court orders in the lines of criminal investigations or criminal instructions." In that sense, the Constitution only refers to public bodies in the realm of enforcement and criminal law. There is no mention of national security and intelligence activities.

Unlike many countries that concede investigative powers to intelligence agencies, the Brazilian Agency of Intelligence (ABIN) lacks the legal authority to interfere with privacy and fundamental rights. For example, the Canadian Security and Information Service (CSIS) has legal support to conduct wiretapping based on the so-called CSIS Act of 1984. This Act limits the type of activity that might be investigated, the ways that information can be collected, and who may access the information (i.e. espionage, sabotage, political violence, terrorism, and clandestine activities). The CSIS Act prohibits the Service from investigating political actions of lawful advocacy, protest, and dissidence. The CSIS can only investigate these types of actions if they are linked with threats to Canada's national security and only after judicial authorization.

In the case of Brazil, the creation of the ABIN in 1999 did not equalize the mechanisms for internal and external control of intelligence. As we have shown in the previous sections of this Chapter, the internal control is promoted by the "Corregedoria" (internal inspection office), whereas the external controls are conducted by the Mixed Commission of Control of Intelligence Activity (CCAI). According to Article 6 of Law 9,883/99: "The external control and supervision of the Intelligence activity shall be exercised by the Legislature in forms to be established by the National Congress". There is no mention of the judicial control of the ABIN. Hence, two scenarios can be drawn regarding the interference of fundamental rights such as privacy. In the first scenario, the Brazilian intelligence has no legal authority to interfere with those rights and abide by the rule and does not undermine or violate these rights. A scenario that is difficult to believe as we attested in the deviations and misuses of intelligence in the previous sections. In a second scenario, the Brazilian intelligence interferes with those rights, despite the inexistence of judicial authorizations, and when it does, the agents are guided by informal lines of effectiveness and optimization of results (i.e. few resources to obtain more intelligence products). In other words, is up to the intelligence services to measure and apply, by their own criteria, the principle of proportionality or reasonableness; balancing between means and ends when interfering with fundamental rights.

However, intrusive actions must weight even in the application of informal methods. Thus, interferences must be justified by the principle of proportionality in every circumstance. According to Lenza (2010), in order to apply the principle of proportionality, three elements are indispensable:

> a) Necessity: the measure to restrict rights is legitimate only if is indispensable to the concrete case. Besides, the measure cannot be replaced by less intrusive actions. This emulates the logic of "lesser evil".
>
> b) Adequacy: the measure is optimal to reach the objectives of the operation. This emulates pertinence or suitability.
>
> c) Proportionality in the strict sense: The executor of the action must weigh if the measure, in terms of adequacy, exceeds the restriction and interference of other values. This entails the notion of maximum effectiveness and minimum restriction as extremes that should be balanced to achieve a certain goal (Lenza, 2010, p. 8).

By analogy, a cautious operational manager of intelligence should follow the principle of proportionality or reasonableness to choose the line of action in a particular case. Regarding the points of necessity and adequacy, we can consider again the example of fundamental rights protected by the Constitution. In Article 5, for instance, there is mention of fundamental civil rights such as freedom of expression, freedom of movement and association, right to intimate life, and right of privacy. By the Brazilian Constitution, one can differentiate intimate life and privacy by affirming that the former is related to the subjective sphere and the intimate treatment of individuals, family, friendship, and close social bonds. In turn, privacy involves the previous dimensions plus objective human relationships, such as commercial, work, and professional relationships. Therefore, privacy encompasses intimacy or intimate life. However, such a distinction is hard to be found in a strict sense.

In terms of the right to privacy, Article 5 of the Constitution mentions that "The intimate life, privacy, honor and image of people are invulnerable; [the constitutional order] assures the right to compensation for material or moral damages resulting from violation to these rights". In light of that, the general protection of privacy entails other specific rights, such as the inviolability of home and inviolability of communications. In other words, the protection of the right to intimate life and privacy in the Brazilian Constitution unfolds into the protection of three categories of privacy: 1) general (image, data, information, etc); 2) home or domicile; and 3) communications. The categories are based on international Law and Treaties signed by the country in the last decade such as the International Treaty on Civil and Political Rights, established by the General Assembly of the United Nations in 1966, and signed by Brazil in 1992. Another example is the Inter-American Court of Human Rights Treaty (CADH) signed in 1969 and ratified by Brazil in 1992. The CADH also establishes similar principles for the protection of

honor and human dignity expressing that "no one shall be subjected to arbitrary or abusive interference in his private life, family, home or correspondence, as well as to unlawful offenses against the honor or reputation" (Art. 2, CADH).

In addition, the Brazilian Civil Code from 2002 (articles 20 and 21) reinforces privacy provisions, enacting sanctions in cases of violation by public or private agents. On the other hand, Access to Information Law (Federal Law 12.127/2011) protects personal information related to intimacy, privacy, and honor and image of persons (article 31). Several public bodies process this kind of information in their databases, such as name, filiation, address, occupation, income, assets, medical reports, legal disputes, etc. We will return to this point in Part 3 of this study. Law 12.127/2011 also establishes a period of 100 (one hundred) years of restricted access to personal information. This information can be disclosed before this time only by explicit consent from the entitled owner of the information (article 31). As a result, the government should take all the necessary means to ensure confidentiality. However, the Access to Information Law removes consent for the disclosure of personal information in some cases, such as in statistics and scientific research, medical prevention and diagnosis, judicial orders, human rights, and protection of the public and general interest (Article 31.3).

Moreover, Article 7 of the Law 12.127/2011 stipulates exceptions to the principle of transparency of the administration. Those exceptions are documents and administrative acts classified as confidential. Article 23 also lists the exceptions to classify information in Brazil:

> Article 23. Information deemed to be essential to the security of the society and the state shall be classified as its disclosure may jeopardize, endanger, harm, or risk:
>
> I - the national defense and sovereignty or the integrity of the national territory;
>
> II - the conduct of negotiations and the international relations of the Country; […]
>
> II - life, safety, and health of the population;
>
> IV - the financial, economic, and monetary stability of the country;
>
> V - strategic plans or operations of the Armed Forces;
>
> VI - scientific and technological research and development projects, as well as systems, assets, facilities or areas of national strategic interest;
>
> VII - the security of institutions and high authorities (national and international) and their relatives;

> VIII - intelligence activities, and criminal investigation and procedures related to the prevention or repression of offenses (Art. 7 Law 12.127/2011).

Point VIII is of special interest in this study as it also covers criminal investigations. This topic is also covered by confidentiality in the Code of Criminal Procedure. Nevertheless, the strategic intelligence activity developed by the Federal Police, which does not relate to the criminal investigation, is also covered in subsection VIII. Finally, the SISBIN and ABIN activities regarding strategic intelligence to the state can be covered by all the subsections of that list.

The subsections above mean that the exceptions to transparency are plenty, entailing a considerable leeway to protect or classified information in the country. Nevertheless, confidentiality to protect personal information should not be put at the same level of confidentiality to protect the security of society and the state.

In the last case, information can be classified into three categories: reserved, secret, or top secret. The time restriction to access those categories is five, fifteen, and twenty-five years, respectively. The latter may be extended for an equal period of twenty-five years once (Article 24.2, Law 12.127/2011). The degree of confidentiality is based on the risk or potential damage that the information could cause to the security of the state if accessed by unauthorized persons (including the public). The maximum restriction corresponds to higher risks. In addition, the expiration date of confidentiality is issued according to the "sensitivity" of the information. As mentioned above, Law 12.127/2011 expresses that information related to intimacy, private life, honor and image of people have restricted access for a hundred years and do not depend on the above degrees of classification. In this case, documents can be accessed only by the person related to the information, or by authorized third parties.

The "ultra-secret" category (restricted during 25 years) is a prerogative of the President of the Republic, the Vice President of the Republic, the Ministers of state and authorities with the same ranks, the Military Commanders (Navy, Army, and Aeronautics), and the Heads of Permanent Diplomatic and Consular Missions. Ultra secret documents secrecy can be extended for another period of 25 years. In the "secret" category (restricted for 15 years), there is no permission to extend the expiring date of the documents. This category can be established by the same authorities who classify the information as ultra-secret, as well as by the leaders of municipalities, foundations or public companies, and companies of a mixed economy. Finally, "reserved" information is confidential for five years, with no possibility of renovation. Authorities exercising managerial or administrative duties, in accordance with the specific regulations of their organizations, might use this category as well as the authorities mentioned in the other degrees of secrecy.

By those categories, the products of intelligence are an exception to the constitutional rule of publicity and are regulated by the principle of secrecy. In the same sense, Law 12.127/2011 establishes that classified documents cannot be added to investigation procedures without judicial authorization. This determination exists because the Federal Supreme Court (Summary Resolution 14) establishes that the attorney in the interest of the defendant has the right to access all the evidence attached to the investigation. To avoid that access, reserved, secret and ultra-secret documents are not considered as prosecution evidence.

Moreover, the violation of secrecy by public agents might be sanctioned according to Article 325 of the Penal Code. In the administrative domain, improper disclosure of personal information by a public agent is considered as "unlawful" conduct or serious military transgression when committed by a member of the Armed Forces. In the case of federal public agents, that disclosure entails suspension and prosecution according to the Law of Crimes and Responsibilities (Law N. 1,079/1950). In the case of personal information held by private individuals or entities, the Law on Access to Information (Law 12.127/2011) does not apply. However, article 2 expresses that "non-profit entities that receive public funds from the national budget or through social subsidies" are submitted to public regulations and controls.

On the other hand, access to archives from the period of the military dictatorship (1964-1985) is still a controversial point. Currently, Law 12,527/2011, in article 30, the item I, establishes that the Commanders of the Navy, the Army, and the Aeronautics have the prerogative of using the ultra-secret category. Thus, the Armed Forces have a legal power to enclose and deny access to their documents. We remind that the expiration date of 25 years is established during the creation of the document (some of the documents of the dictatorship could have been classified during the transition or in the democratic era) and can be renovated once. The historical archives of the SNI, as well as from the military intelligence were transferred to National Archives. However, during the dictatorship period, Decree N. 60,417/1967 and Decree N. 79,099/1977, which are still valid to manage the safeguarding of confidential matters, established the destruction of the documents according to the criteria of the authority who supervised the archives. Thus, the National Archive released 40 reports accusing the destruction of almost 20 thousand documents from the SNI (Carpentieri, 2016). The remaining documents were lost, stored in private deposits, or are still classified according to the regulations of the Law on Access of Information. Hence, these limitations to access historical records characterize the Brazilian scenario and they were exemplified in the work of the "Truth Commission" (see Section 3.2); a civilian commission that elaborated reports about the torture and missing persons during the dictatorship. The commission was accused by the Military by being ideologically biased and for revealing doubtful information. Yet, when the Armed Forces were invited to support and collaborate with the commission, the

military commanders refused to declassify information that could have changed the historical memory from those times (Pereira, 2015).

When it comes to judicial control, we mentioned that, in Brazil, the ABIN has no legal jurisdiction to intercept or interfere with fundamental rights enshrined in the Constitution such as intimacy and privacy. Thus, that lack of regulation blurs the borderline between the strategic intelligence developed by the ABIN and the police intelligence conducted by enforcement authorities. The result is that, sometimes, the activities of both domains overlap and compromise their results. In the previous section, we have shown that the Satiagraha case of corruption was just an example of overlapping jurisdictions between the ABIN and the Federal Police to prosecute financial crimes. In this case, the proof against bankers who committed white-collar crimes was revoked because ABIN agents collected proofs with no judicial warrants. The cancelation of the process is legitimate since no intelligence and security institution should be able to collect and prosecute targets by extra-judicial means. From 2008 to 2012, this raised a series of inquiries by legislative commissions (see the previous section) in order to scrutinize the investigative role of ABIN agents. Despite those problems, the current legal configuration expresses that the interference of fundamental rights to support an investigation is only circumscribed to enforcement institutions such as the police.

In the case of the Federal Police, the intelligence gathered and disseminated to policy-makers have different categories (information, estimative scenario, appreciations of risks).[58] However, those reports are administrative and cannot be "attached" to judicial investigations and prosecutions. Yet, information from those reports could be shared with other police agents to support the collection of evidence and the investigation of crimes. Those reports can also be shared with strategic intelligence services (ABIN-SISIBIN). To share these documents, the dissemination of intelligence is linked to restrictions. For example, the classification is always essential as a counterintelligence mechanism because it restricts the audience to whom the information is directed. The use and classification of those reports are classified according to the Penal Code in the realm of criminal law. On the other hand, public safety institutions, such as police agencies, might access to public information and personal data related to names, affiliation, addresses, electoral situation, and administrative records maintained by public entities. This is because this kind of data is understood as less sensitive in terms of privacy rights. Moreover, the analysis and collection of these data are

[58] The result of the evaluation is sorted according to its content and sources. The source will be classified into one of six categories: A: entirely suitable; B: normally suitable; C: regularly suitable; D: normally reliable; E: reliable; and F: could not be evaluated. In the same logic, the content will be assessed as 1: confirmed by other sources; 2: probably true; 3: possibly true; 4: doubtful; 5: improbable and 6: could not be evaluated (BRAZIL, Ministry of Justice, National Secretariat of Public Security, Ordinance No. 22-SENASP, approves the National Doctrine of Public Security Intelligence - DNISP. Official Bulletin of the Union, Brasília, DF, year 146, ed. 139, 23 Jul. 2009. Section 1, p. 26-27).

allegedly essential to security tasks. For example, in the case of telephone communications, the restricted access to telephonic data should not be mistaken with the secrecy of telephone communications, protected by the Constitution. The former data consist only of the log and metadata of the connections and does not demand judicial authorization to be accessed by security agencies (including intelligence services). The latter data relates to the content (the "real" data) of the conversations and requires judicial warrants to be accessed by security agencies (except by intelligence agencies).[59] Law on Criminal Organizations also defines that telecommunication providers should keep logs and metadata for five years (Article 17). If requested, this data should be transferred to police officers and members of the Public Ministry, implying that judicial warrants are not necessary for metadata. However, keeping telephone records for such a long period increases the chances of improper access. The same applies to Internet access logs, with the difference that the expiring date is for six months (Brazilian Internet Civil Framework, article 15). In the case of intelligence services, they are able to request metadata from administrative and judicial bodies in terms of cooperation or to conduct their security duties. However, the data requested can only refer to metadata and to information that does not extrapolate the missions of intelligence. However, if the intelligence service, in practical terms, sometimes deviates from norms and regulations governing the interference of privacy and fundamental rights, in our vision, the authority to allow such deviations must be regulated and protected by law. Despite the dilemmas that might arise because of this kind of regulation, maybe similar to the ones related to the Prior Judicial Control of the Spanish intelligence, this is a point worthy of consideration in Brazil.

In that sense, there have been attempts to fill the gap to establish judicial control over the Brazilian Intelligence System (SISBIN). Due to the continuous monitoring of political parties during the 90s, of social movements during the 2000s (see the section of Internal Control), and after the operation Satiagraha, Legislative representatives had discussed the best forms to establish a Prior Judicial Control of intelligence. One example is the proposal created by Deputy Jô Moraes, who was also President of the Commission of Control of the Intelligence Activity (CAAI). Law Proposal N. 3.578/2015 by Moraes aimed to establish the procedures and means to implement judicial control over the ABIN. The proposal would have enabled the use of new techniques (from the legal perspective), such as the use of secret interviews, operational recruitment, infiltration, surveillance, interception, or capture of images, data, and signals. The agency would need to report all the actions, methods, and operations that interfere with fundamental rights (intimacy, privacy, and inhuman treatment) to the Judicial power (Articles. 3-5 of the proposal). The ABIN would need to write and communicate precise and

[59] The jurisprudence of the Federal Supreme Court (STF) issues that breach of confidentiality of telephone data can only happen by means of judicial authorization or petition by a Legislative Commission of Inquiry (CPI) within the National Congress, or in one of the Houses, according to the investigative power of the judicial authorities based on art. 58 of the Federal Constitution.

detailed statements about the situation, mission, means, technique, resources, coordination, control, evaluation, and, finally, the limits of the performance of the intelligence actions. This control aimed to evaluate the need, adequacy, and proportionality of intelligence measures defining that the interception of private communications (Article 8), violation of home (Article 9), and infiltration in target groups (Article 10) only could be executed through prior judicial authorization. The actions would have needed to justify if there were alternative means or techniques to collect information as well as the urgency to conduct the operation. Finally, one Authorized Federal Judge would need to weigh whether the justification is sufficiently relevant to authorize the means and techniques required to interfere with fundamental rights and constitutional norms. In other words, the proposal follows the three proportionality principles mentioned above (necessity, adequacy, and proportionality) to enact judicial control. However, since the Legislative power weakened its role to oversee intelligence issues during the last years (see the history of the CCAI Commissions in the previous section), the Executive Board of the House of Deputies dismissed Moraes proposal in January of 2019. Judicial control, hence, still waits to be developed.

Intelligence services, as well as any other state administration, must be integrated into the Constitution and cannot be an exception to the principle of legality or the predominance of constitutional terms. This logic, which in principle recognizes certain rights and limits, is articulated through the separation of powers. In the Rule of law model, the relationship between the holders of political power and the subjects of that power is mediated by legal norms, that is, the exercise of power is limited and subordinated by the public law. On the one hand, the sovereign power allows the state to maintain certain operations based on secrecy and security grounds, a trend intensified in the face of new and complex threats. On the other hand, legitimacy of that power is created by mechanisms of horizontal accountability, which consists of recognizing that there is not legitimate sovereignty (even if it protects subjects against complex threats) without control and scrutiny. Therefore, in the balance between state secrecy and publicity, there must be a preference to establish judicial controls and legitimate forms to authorize the interventions of sensitive data and rights, in order to ensure the protection of the state and the population.

In addition to matters related to state secrecy, such as the use and access to sensitive data, the judicial control of intelligence might involve prior authorization for actions that restrict fundamental rights. As shown above, those situations are more common in investigative procedures that require criminal intelligence. In some countries (i.e. Spain, Canada, Australia) this type of control can be authorized by specific judges with competence for such situations. In other countries (as in the case of Brazil), a considerable problem of judicial control emerges if we consider that the Brazilian scenario is notorious by different deviations in the intelligence activity such as overlapping of functions with other security organizations, the

universe of clandestine investigations and their commercialization, and the indiscriminate use of judicial orders to authorize telephone wiretapping to the police (Carpentieri, 2016). In short, those actions are forms of governmentality in which the exercise of the power of intelligence is not regulated by legal lines. Yet, this power can potentially be executed with a considerable degree of informal autonomy that must be addressed.

Epilogue

To conclude this section, let us reconsider the forms to classify information and the dilemmas to disclose it by judicial means. In that sense, according to Bayer (2010), one of the big problems related to the exchange of information in security domains is the culture to classify all kind of information, a culture that, in the case of intelligence, resembles a logic of the Cold War. To him, over-classifying information decreases the level of coordination and cooperation, and makes it inaccessible in circumstances in which it would be extremely necessary. Moreover, according to Bayer, when classifying any kind of information becomes the rule, "interest to disclose is aroused as secrets are transformed into objects of desire that eventually would be leaked" (Bayer, 2010, p. 57).

To avoid the problem of over-classification, it is essential to think in advance the restricted audiences that can use it for legitimate purposes, such as Parliaments and Courts. In that sense, Bayer shows some ways that would promote a reversal of the widespread logic of the Cold War period, which is inadequate to face the complex scenario imposed by the globalization of communication and technology: "not to classify information unless there is a concrete probability of this knowledge to cause damage to national security" (Bayer, 2010, p. 52). Although the term "national security" is obscure, the author argues that information should not be classified in these terms: a) to promote or mask legal violation and administrative inefficiency; b) to prevent the embarrassment of a person, organization or agency; c) to prevent competition between organizations or; d) "to prevent or delay the release of information that does not require protection in the interests of national security" (Bayer, 2010, p. 59).

By denouncing the culture of over-classification, Bayer attests that, although the intelligence community claims this procedure with the discourse of protecting sources and methods, and the police invoke the protection of investigations, there are many occasions to encourage disclosing and cooperation. "Classification is typically a political decision, not a technical action" (Bayer, 2010, p. 53). To revert this, Bayer proposes to replace classification by the categorization of sensitive information. To him, the exchange of sensitive information would stimulate a secure environment to share data because: "a) information circulating without classification labels would avoid the fetishistic desire to disclose it; b) there is less concern of "burning cases" or compromising the sources when information is

leaked; and c) law enforcement and security information are protected by law and its leakage is considered a crime" (Bayer, 2010, p. 53). It is important to notice that careful sharing is different from eliminating the circulation of information. The use of the above-mentioned criteria provides tips for transforming the categorization of information from classified to sensitive. Yet, in our view, in the case of counter-intelligence measures, the use of classification labels (reserved, secret, ultra-secret, or top-secret) is still valuable but must be carefully used.

All the same, in this section we have mentioned that one of the main dilemmas for the judicial control of intelligence in Spain and Brazil is to access huge amounts of classified information in the hands of the Executive.

In Spain, the Constitution expresses publicity and transparency as principles to be projected on the three branches of the state, being a structural demand for the Rule of Law and to guarantee the exercise of rights and freedoms of citizens. Yet, the administration can deny access to information and transparency when documents contain information on acts of the Central and Autonomous Governments or matters related to national defense or state security; indicating that the culture of over-classification is normalized in this domain.

Moreover, in Spain, many administrative and intelligence documents were hidden or destroyed without any legislation for consultation or clarification since the end of the Franco regime. When the documents are stored in public archives, the access to those files is permitted under criteria established by the Official Secret Act (LSO) and Historical Heritage Act, which established hard declassification rules or inexistent criteria to declassify historical documents from the longest past (before the constitutional era in 1977). Therefore, Spain needs a new legal framework to adequately manage the dilemma between transparency and security in the management of historical and public affairs (Matey & Guisado, 2019).

In the case of intelligence, the CNI has the mission to obtain, evaluate, interpret, and disseminate the necessary information to protect and promote the political, economic, industrial, commercial, and strategic interests of Spain. Even if those missions are not mistaken with espionage, the CNI can suspend and interfere with constitutional principles (publicity, dignity, non-interference of communication, and so on). To do this, the intelligence service should take into account that there are no other less aggressive means or methods to achieve end goals. Finally, when intelligence interferes with those principles, there must be proportionality in this action, as a judge needs to weigh the seriousness of the interventions and the reasons that justify them.

However, despite the need for prior judicial control, some critiques have emerged in the Spanish case. For example, in different moments, it has been pointed out that this kind of control provides a veil of legal appearance to the

activities carried out by the CNI, rather than to consolidate an authentic and substantial control. We mentioned that this control is based on the European jurisprudence, and it might be deepened and strengthened if more Magistrates – not only one- oversee the activities and the measures that are requested by intelligence. Another critical point is that the nomination of the judge responsible for the intelligence control follows special criteria in the Magistrate Court; transmitting the idea that the CNI owns a favorite magistrate, either by prior selection or by indicating one "a la carte". Furthermore, the rule allows the Director of the CNI to provide minimum information standards to the judge. This puts into question the real ability of the Magistrate to weight the proportionality of intelligence interferences over fundamental rights. The legislation is also not clear in cases in which the Magistrate rejects proposals that are not fully justified. In addition, after the judge authorizes interventions, he/she does not supervise the deletion of information (especially the data not related to the interventions) and cannot verify whether the authorization has been respected and followed. That is, the main deficit of this *a priori* mechanism is that it cannot reach other phases and procedures of the intelligence activity. For Pérez-Villalobos (2002), this makes the authorizations to become a purely formal act, and not a real and effective judicial control. Finally, there are no satisfactory institutional and legal channels to receive complaints of persons whose fundamental rights and freedoms were interfered or suspended by errors or intelligence mistakes.

In the case of Brazil, the only way to access classified information is waiting 100 years in case of documents with personal information that could affect the intimacy, private life, honor and image of individuals; except when information is processed in statistical, research and administrative tasks. In these cases, classified information receives three categories: reserved, secret, or top secret. The restriction to those categories consists of five, fifteen, and twenty-five years, respectively. The latter one might be extended for an equal period of twenty-five years (Article 24.2, Law 12.127/2011). Thus, in contrast to Spain, the Brazilian scenario has regulations to disclose official information. However, the case of Brazil is even more problematic since there is no judicial control of the ABIN-SISBIN.

Regulating this control is a controversial point since the Brazilian scenario is notorious by different deviations in the intelligence activity such as overlapping of functions with other security organizations, the universe of clandestine investigations and their commercialization, and the indiscriminate use of judicial orders to authorize telephone wiretapping to the police (Carpentieri, 2016). In short, all those actions are forms of governmentality in which the exercise of power in intelligence is not regulated by legal lines but is exercised with a considerable degree of informal autonomy. Yet, a basic legal ground should be laid insofar as intelligence could interfere *de facto* with fundamental rights; a situation that demands, thus, a priori control to justify proportionality in the strict sense. To

achieve this, the controller of intelligence must weigh if the intervention exceeds the restriction and interferences of rights. This entails the notion of maximum effectiveness and minimum restriction as extremes that should be balanced in intelligence activities.

Both in Spain and Brazil, intelligence cannot be a *carte blanche* to override fundamental rights. Intelligence should be understood as an exceptional measure to suspend those rights in order to protect them. With this, the dilemma between intelligence (and security by extension) against fundamental rights (and democracy by extension) could be solved as they are not antagonist sides of a clash. Rather, the former is operationalized to simultaneously suspend and preserve the latter. Suspending freedom of information, for example, constitutes a necessary measure to sustain a society of rights and plural information. In short, the suspension is contingent and limited by the own teleological principle of sustaining and enabling the proliferation of a space in which civil rights are practiced and exercised despite the threats embodied by external circumstances or the side-effects from the rules that protect them. This argument was made very clear when the Constitutional Court of Spain, in its Judgment 31/2014 of February 24, considered that the classification of a matter (and intelligence activity) "cannot suppose a space of immunity to judicial control" (Barrilao, 2019, pág. 318).

In both countries, the courts should react in cases of indiscriminate eavesdropping and regulate electronic mass surveillance by intelligence, as those services cannot execute actions without warrants and by indiscriminate means and objectives. Moreover, the courts should control and verify the targets of intelligence. That is, the judicial control should be able to limit the type of activity that might be investigated (i.e. espionage, sabotage, political violence, terrorism, and clandestine activities), the ways that information can be collected, and who may access the information. At the same time, they should rule a line that cannot be crossed when it refers to investigating political actions of lawful advocacy, protest, and dissidence. Leaving the leeway to decide all of those activities to the intelligence services implies in promoting a form of action that suspends accountability and supports a power with the capacity to decide upon the different threats and menaces to the country. There should be a line to check the power and the objectives of intelligence; a kind of human activity that deliberately (or accidentally) can misunderstand certain actions that not necessarily represent real threats to the country. As intelligence cannot always differentiate the array of phenomena and threats, the Courts should set basic lines and implement controls beyond the elaboration of *a priori* authorizations and warrants.

However, in that supervision, the courts and judiciary can be reduced as a control mechanism vis-à-vis intelligence through the problem of judicial deference. Even in democracies with active judicial power, the courts have traditionally shown deference to the executive branch on issues concerning national security.

Equally harmful is the absence of an autonomous judiciary. Judges who are subject to political influence and pressures may be unable to function effectively in their overseeing function (Caparini, 2016). In that sense, as in the case of the legislative control of intelligence, judicial courts can work together with independent bodies to enhance higher levels of accountability. For example, the office of ombudsman may be granted the power to investigate and report on a complaint made by the public against the intelligence services. The ombudsman is an independent official who investigates on behalf of the complainant, usually focusing on procedural and administrative issues rather than on judicial matters, and he/she usually ends with a recommendation to solve a problem rather than a binding remedy (Born & Leigh, 2005). Another type of independent oversight body is the national audit office, which is independent of the three branches of government in many countries but reports to the legislative. An effective audit office is not only responsible for the financial control, but also for "the performance and efficiency of internal projects in terms of financial policies and managerial evaluations" (Born & Leigh, 2005, p. 113).

So far, we have expressed the main aspects of the judicial control of intelligence. Those aspects are summarized in Table 11. At this point, what are the overall accountability mechanism and values enhanced by the role of courts?

In Spain, the CNI is accountable to the judicial power through Act 11/2002. According to it, the strategic and national security activities of the CNI that interfere with fundamental rights need to be reported to a Magistrate Judge of the Supreme Court to obtain *a priori* authorization and warrants. Fundamental rights that must never be suspended are life, and non-degrading treatment (absolute and universal rights). In turn, there can be contingent suspension of the inviolability of the home, and secrecy of communications. Yet, the Spanish Magistrate has no capacity or jurisdiction to authorize the interference regarding the honor of persons, family/personal privacy, personal data rights, and the potential use of electronic and mass surveillance that interfere with those rights. The Spanish jurisdiction protects those rights, yet, they are partially developed or not mentioned in the prior judicial authorization of the intelligence activities. In the cases that the CNI interfere with fundamental rights, the Center needs to justify the motives to suspend those rights, identifying the targets, formulating the proportionality of the interference (adequacy and objectives), indicating the time/location of the measures, and the renovations of the interference if it is necessary. There are no mentions to a posteriori assessment and elaboration of statistics to the public (reports). We recommend creating this kind of report, similarly to the ones released by technological and telecommunication companies that publish the volume of data requests and warrants presented by enforcement agencies (see Chapter 5).

In the case of Brazil, the ABIN and SISBIN organizations have no capacity or legal authorization to interfere with fundamental rights from the Constitution, such as life, intimacy, privacy, the honor of persons, inviolability of the home, the secrecy of communications, or to conduct actions related to electronic and mass surveillance. In that sense, the Brazilian scenario has not established clear judicial lines that cannot be crossed by the services.

Table 11: Accountability in the judicial control.

Accountability dimensions	Cases	
	Spain	Brazil
Who is accountable?	National Intelligence Agency (CNI)	Brazilian Intelligence Agency (ABIN) as coordinator of SISBIN
To whom are they accountable?	- To the Judicial Branch, through act 11/2002	N/A
About what are the services accountable?	Strategic and national security of the state activities that interfere with fundamental rights; Absolute: - *Life,* - *Non-degrading treatment* Suspension: - *Inviolability of home* - *Secrecy of communications* Non covered in its integrity: - *Honor of persons* - *Family/personal privacy* - *Personal data rights* - *Electronic and mass surveillance*	The intelligence services have NO legal warrant to interfere with the fundamental rights of the Constitution, such as: - *Life* - *Intimacy* - *Privacy* - *Honor of persons* - *Inviolability of home* - *Secrecy of communications* - *Electronic and mass surveillance*
How are they accountable? (measures)	Justifying the suspension of rights to obtain a priori judicial authorizations considering - Identification of targets - Justification or motive - Proportionality - Time/Location - Renewal of the interference - Evaluation and reports (?)	N/A
Assessing accountability according to its internal principles	Did the accountability action result or promote at least one of the following principles? -Responsibility ~~-Answerability~~ -Enforcement (punishment) ~~-Transparency~~	Did the accountability action result or promote at least one of the following principles? ~~-Responsibility~~ ~~-Answerability~~ ~~-Enforcement (punishment)~~ ~~-Transparency~~

Source: author

According to our methodological operationalization, the performance of public accountability as a connector between authority and legitimacy is a question of interest. When authority is called to give an account, if that action does not entail more legitimacy, then accountability fails to reach its objective. In that logic, when an authority from intelligence is called to be accountable by judicial means, it is possible to speak of accountability by responsibility and enforcement. When intelligence authorities show responsibility (by fulfilling the duties and measures to them conferred), accountability turns up creating new sources of legitimacy by reconsidering the people that authority is supposed to represent. By showing responsibility and representing indirectly the voices of citizens after elections and formations of governments, this basic form of accountability creates the conditions to perpetuate the very intelligence procedures and institutions as well as the sociopolitical order as a whole.

Moreover, when an intelligence authority is called to be accountable before the courts, what is primarily called is an attachment to justice and the protection of fundamental rights of citizens. In this case, the courts could enforce the disclosing of classified information, the legal lines to temporarily suspend certain rights, and establish sanctions via administrative and criminal Law. For example, the courts can react to the violations of rights, the misuse of funds, and the unauthorized access to official information. In closed doors meetings to request classified information to assess the Executive, or in the mission of specific judges to authorize intelligence operations, this kind of accountability relates to check and balances and the division of powers. Besides, the role of courts complements other forms of accountability. For example, different accounts can be demanded of the same authority, such as initial justification of responsibility by internal controls, as well as answerability actions promoted by Parliament Commissions. These actions might be followed by sanctions or intervention of courts. However, the enforcement principle of accountability (punishment) is sporadic and depends on the clashes between the Judicial and Executive branches to solve issues such as the interpretation of secrets; and is scarcely used in institutional forms, such as in the evaluation of the authorizations that interfere with fundamental rights. In the latter form, the warrants and legal coverage for intelligence operations seek to restrain the impetus or initial action of the Executive power, rather than evaluating and correcting (even by punishment or sanctions) the collateral damage that this power can inflict during or after intelligence operations.

If courts obtain more evaluation capacity to assess intelligence operations, then legitimacy will be called to be a product of accountability. In this case, accountability by courts would promote justice and citizens' rights. This is because an authority that is accountable before courts can show respect to norms but also promote legitimacy and develop societal values beyond formal procedures. In this case, courts would demand legal respect to the jurisprudence and constitution, as well as enhance better protection of rights and restore justice. In this sense, after

abuses of power, authoritarian experiences, and over-interference in individual and civil liberties, Justice would be promoted as the main value of an accountable action.

Finally, in terms of independency of courts, the problem of judicialization of politics was not verified in the field of intelligence. The agencies of the Spanish Executive have veto power (*potestas*) to block the influence of the courts, and there is no judicial control of intelligence in Brazil. However, the reversal problem, the politicization of justice, might arise in the forms that the Executive appoints the criteria to select the Magistrate judge who is supposed to control intelligence. This trend might also be promoted insofar as the Executive over-classifies information and regulates the flow of accounts to external bodies. In that sense, as mentioned, justice needs collaboration from unusual sources in order to be reinforced. One of these sources is the role of international organizations and supra-national bodies: the so-called accountability of "third dimension".

3.7. Accountability of third dimension

There is another form of accountability called the third dimension. This refers to the role of international players and arenas to promote accountability beyond the vertical and horizontal dimensions. This is the case, for example, of international movements, supra-national courts, multilateral organizations, and transnational associations.

In the theoretical framework, we stated that accountability is a concept with multiple directions. For example, O'Donnell (1998) gives a distinction between horizontal and vertical accountability. The former is related to a relation of "equals" between institutions or individuals in a chain of power. One classic example is the checks and balances between governmental branches. The latter refers to promote accountability in a relationship of asymmetric power, for instance, when superior ranks account to lower ranks in a hierarchy, or when the civil society asks for justifications of policymakers in the context of a public decision. And third dimension, in turn, would refer to a mix of vertical and horizontal accountability that comes from parallel scenarios, such as international arenas.

In light of that, as a case of accountability of the third dimension, we can consider the impacts and forms to oversee the international integration and cooperation between intelligence agencies. The official cooperation in this realm had started during World War II and the Cold War. Since 9/11, there has been an exponential increase in both the scope and scale of intelligence cooperation between states. In particular, the fight against international terrorism has provided a considerable increase in multilateral and bilateral intelligence agreements. The growth of international phenomena, such as organized crime, the proliferation of money laundering, cyberattacks and cyberwarfare, and so on, has entailed tight cooperation between intelligence services in many states to meet these challenges. However, cooperation in terms of intelligence present special characteristics and sometimes is very poor (Born, Leigh, & Wills, 2011). The need for preserving sources and operations makes the information to be filtered by the sending organization and kept in secret by the receiver part. Cooperation between the different services, even within the same country, might be poor or uncoordinated.

Bilateral cooperation between countries and multilateral cooperation present special characteristics. For instance, Westerfield (1996) has suggested that intelligence services are used to establish liaisons but, in practice, cooperation has no obvious single place or location. Despite this, Westerfield offered one of the first taxonomy of intelligence cooperation, identifying at least six possible forms: fully-fledged liaison; intelligence information sharing; intelligence operations sharing; intelligence support; crypto-diplomacy, and the intrinsic risks of liaison (such as

uncovering or dissolving intelligence operatives deployed in the ground) (Westerfield, 1996, p. 529). He also distinguishes informal or ad hoc cooperation and 'fully-fledged liaison' or official and formal cooperation. In both forms, intelligence services emulate the diplomacy of their states, constructing treaties and exchanging 'liaison officers', who are similar to ambassadors. This ensures that intelligence services recognize international sovereignty and jurisdiction. Typically, such treaties specify that the parties cannot recruit each other's citizens as agents without permission or operate on the foreign territory without prior approval. In other words, even in the world of intelligence, practitioners use professional codes and establish (in)formal mechanisms of cooperation at the international level.

In the case of Europe, intelligence cooperation is reflected in many of the treaties and multilateral agreements in this realm. For example, after the Al Qaeda bombings in Madrid (2004) and London (2005), the European intelligence and security services resolved to provide a framework for cooperation and a link with the United States. The so-called "Club of Berne" is a longstanding group that integrates the EU heads of state security and directors of intelligence, plus the ones representing Norway and Switzerland. The Club meets on a regular base to discuss intelligence and security matters of all kinds. After 9/11, the Club of Berne created a second body, the Counter Terrorist Group (CTG). This functional organization has served as a focus for cooperation and has provided threat assessments to key EU policymakers drawing on national resources. The CTG promotes broad intelligence convergence rather than the mere exchange of information. The Group can be considered as a forum of experts that develop practical collaboration on particular projects and joint methodologies (Born, Leigh, & Wills, 2011). By joint methodology, the Group allowed European countries with more experience in antiterrorism to share skills and techniques, as well as the standardization of procedures (CTG website). A third multilateral body for intelligence cooperation in Europe is "The Special Committee of NATO". This integrates the heads of the security services of the North Atlantic Treatment Organization. The Committee was formed in the early 1950s and, after the Cold War, its role was mostly modified to address the difficult security problems on sharing sensitive military documents amongst NATO's growing membership, as in the case of Spain integration in 1985. After the war in Afghanistan in 2002, the role has been expanded to the Middle East and Eastern Europe due to the enlargement of the EU and the incorporation of new State Members. NATO is the main military intergovernmental alliance in Western Europe and, among different missions, constitutes itself as a front to restrain the Russian geopolitical position and influence in the East.

Despite the multilateral agreements, the European Union has focused on regulatory and judicial matters, instead of seeking to develop a new regional intelligence institution to operate in a permanent role. This kind of operation

emphasizes information and personal data exchange between the Member States, as this material is not highly classified. The EU is less regarded as a common front of unified intelligence, than to a regional space for the multilateral intelligence exchange. However, the prospective trend is to increase data-mining and big data capacities of the current multilateral bodies. In that sense, some scholars have argued that data-mining with no oversight and controls represent one of the most pernicious aspects of the "war on terror" because of the "emphasis on risk management techniques that seek to address security problems by focusing on marginal groups" (Born, Leigh, & Wills, 2011, p. 32). Data-mining is connected to intelligence sharing in many ways. The growth in the sharing of data by states underlines the gradual corrosion of boundaries between domestic and foreign domains. The construction of vast data warehouses raises privacy concerns that are not addressed either by intelligence accountability committees or current data protection guidelines and privacy laws (Delpeuch & Ross, 2016).

On the other side of the Atlantic ocean, the Organization of American States (OAS or OEA), is a continental organization that was founded on 30 April 1948, for regional solidarity and cooperation among member states. Headquartered in the United States' capital Washington, D.C., the OAS comprises 35 independent states in America. In Article 1 of the Foundation Charter, the goal of the member nations in creating the OAS was "to achieve order, peace, and justice, to promote their solidarity, to strengthen their collaboration, and to defend sovereignty, territorial integrity, and independence". Article 2 defines as essential purposes to strengthen the peace and security of the continent, promoting and consolidating representative democracy, with fair respect to the principle of non-intervention. Yet, this principle was not respected as in the case of the USA military intervention in several American countries, including the influence in the Brazilian military coup in 1964. The OAS Committee on Hemispheric Security works on a regular base and comprises members indicated by the executive branch of the State Members. However, there are not permanent and formal channels for intelligence cooperation in this Organization.

Another multilateral space is the Southern Common Market or "Mercosur", a South American trade bloc established by the Treaty of Asunción in 1991. Its full members are Argentina, Brazil, Paraguay, and Uruguay. Mercosur's purpose is to promote free trade and the fluid movement of people, goods, and currency. The Mercosur defines itself as a trade union. Because of that, the Member States exchange information regarding customs, police records, and security information that can be used by counter-part enforcement agencies (Botto, 2015). In that sense, we can speak of basic information exchange that can be converted into intelligence by police agencies in each country. Yet, those channels are not regular and permanent operative intelligence cooperation nodes, as in the case of NATO and the Bern Club.

We have mentioned the organizations and institutional forms for intelligence cooperation in Europe and the Americas. However, what is the impact of international cooperation on accountability?

Intelligence cooperation at the international level is the tip of the iceberg of international policies and geopolitics. International cooperation has in general evaded the scrutiny of national oversight. In overall terms, national bodies to control intelligence were designed in a different era, responding to abuses of power and deviations at the domestic scale. Indeed, as the previous sections suggested, it has become increasingly evident that domestic bodies are ill-equipped to hold intelligence services and their political masters to account for their activities. For example, in the case of Germany, the Bundestag established a Committee of Inquiry in 2006 to investigate the cooperation between German agencies and the USA in Afghanistan and Iraq after the revelation of the CIA rendition flights. In other cases, investigation of allegations involving human rights abuses was also promoted. In Canada, judicial inquiries were created to examine allegations of complicity in rendition and torture, as in the case of Maher Arar and the Federal Court. In Italy, "prosecutors investigated the abduction of Abu Omar from Milan in February 2003 and filed criminal complaints against 22 United States' CIA officials and two Italian intelligence agents" (Born, Leigh, & Wills, 2011, p. 110). However, the prosecution against the agents was not possible due to considerations of state secrecy, and because the USA officials benefitted from diplomatic immunity or were simply out of the Italian jurisdiction.

Those actions can be circumscribed to alleged violations of international treaties of Human Rights. For example, when a state transfers an individual to another state by committing torture or inflicting ill-treatment, it may thereby incur in failed responsibility to fulfill the International Law such as the Convention Against Torture (CAT). In that regard, there is an express prohibition of the use of evidence obtained by torture or ill-treatment in court proceedings contained in Article 15 of the CAT. However, there is no clear international obligation that prohibits a state from receiving or making use of intelligence obtained as a result of the violation of fundamental human rights. In the case of the CIA rendition flights during the War on Terror, it was noted that the purpose of interrogations in most of the cases aimed to obtain intelligence. Yet, it is difficult to assess to what extent a state which is not directly involved in such practices is allowed to receive and make use of intelligence that might be originated by violations. The international law does not address responsibility in cases a state receives or shares information extracted by third states with alleged torture methods. This point is separated from, whether a state that has been involved in such violations (aided or assisted a rendition, arbitrary detention, torture, and ill-treatment of an individual) will assume its international responsibility for those particular acts. In the above-mentioned Italian trial of CIA officials, it was clear that the USA was not interested in collaborating with the courts of the European country. In the Spanish

case, we have shown that the Commission for Reserved Funds of the Parliament received initiatives of representatives to scrutinize the CNI and the Spanish Ministers in the context of the CIA rendition flights using Spanish airports (See Legislative Control section). In most of those cases, the initiatives were simply ignored or expired. When the Government itself presented their motivations to a group of Parliament members, the explanations and motivations for the collaboration with the CIA were presented only after the pressure of the Parliament, international NGOs (such as Human Rights Watch and Amnesty International), a commission of jurists, and investigative journalists. That is, civil society, together with the Parliament, sparkled initiatives of accountability. Yet, the results of the accounts were presented behind closed doors and did not entail further judicial actions as in Italy and Germany.

In terms of accountability, it seems that the Spanish government and the CNI used the argument of plausible deniability of responsibility in the episodes of the CIA rendition flights. In doing so, they used a known tactic that inhibits greater levels of accountability, such as answerability and enforcement, and promoted a reactive logic of extinguishing the fire when the alarm sounds. Denying something that could have happened also avoids learning from wrongdoing and assuming responsibilities to improve international cooperation with foreign services. For instance, plausible deniability avoids legislators and politicians to reformulate the best forms to oversee intelligence cooperation. It is better to assume and learn from mistakes than keep trailing the wrong path.

Since it is difficult to say where complicity with torture starts, the assessment of alleged collaboration with this kind of violation requires a case-by-case analysis but also international standards. In that sense, intelligence agencies do not operate in a legal vacuum. Their actions are attributed to the state in the domain of International Law. The problem is that international legal standards are less clear about receiving information that may have been obtained from torture or interference with human rights. To solve this problem, scholars such as Scheinin & Vermeulen (2011) argue that there is an absolute prohibition to use information obtained from torture (and probably arbitrary detention) in court proceedings. On contrary, Borelli (2003) expresses that "states – and in particular their security services – are not prohibited from receiving and making use of intelligence, whatever its provenance or the methods by which it was obtained". She argues that any "suggestions to the contrary" would "go far beyond from the current situation of the international law" (Borelli, 2003, p. 805). Those ideas reflect that international legal standards in this realm are still debatable. However, given that states are prompt to use controversial (and even immoral) products of intelligence cooperation when the exigencies of national security so require, there can be little doubt that the existing legal framework needs to be readapted continuously (Ganor, 2011).

Another impact of intelligence cooperation is the mass surveillance that might be conducted at the international level. In this matter, a paradigmatic case emerged after the Snowden Revelations in 2013. One of the NSA programs revealed by the former USA intelligence analyst is Prism. Under the Prism program, the NSA allegedly had direct access to personal Internet data and performed intrusive surveillance on online communications storing information such as email, video and voice chat, photos, voice-over-IP chats (such as Skype), file transfers, and social networking content. In order to achieve this capacity, the NSA relied on the collaboration of several companies such as Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, and Apple (Lemieux, 2018). In 2015 a Federal Court of Appeal stated that the bulk metadata collection was illegal, striking down the particular interpretation of Section 215 of the Patriot Act that allowed the government to massively intercept communications of US Citizens without proper constitutional protections. The US Freedom Act was adopted in 2015 to end to bulk metadata collection. However, it is not clear if the new cyber threats, intelligence operations, and mass surveillance legislation really limit the ability of the NSA to gather metadata through third parties.[60] Due to the lack of privacy safeguards in third countries, the EU has revoked and reestablished data transfer agreements with the USA in the last years, such as the 'safe harbor' and 'privacy shield'.[61]

The Snowden leaks included allegations that the NSA was spying on political leaders from USA allied countries such as Germany and Brazil. German chancellor Angela Merkel angrily chastised President Obama for allowing the United States to listen to her phone calls. In the case of Brazil, the former President Dilma Rousseff canceled her official visit to the White House and criticized the NSA interceptions. In her speech in the United Nation in 2013, she also claimed that this kind of "espionage" was a violation of international law.[62] The critiques helped to compel a change in the USA surveillance policy. In January 2014, President Obama announced, "[U]nless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies".[63] In that time, the administration enacted the Presidential Policy Directive 28 on Signals Intelligence Activities, which suggested that the United States limited its existing surveillance to certain states' leaders. The media

[60] Gorman, S. 2006, May 18th. 'NSA Killed System that Sifted Phone Data Legally'. *The Baltimore Sun*, 18, A21.
[61] *DW News*. 2020, July 16. 'EU court overturns US data transfer agreement in Facebook privacy case', retrieved from https://www.dw.com/en/eu-us-data-transfer-facebook/a-54194377 in 07/23/2020.
[62] Borger, J. 2013, September 24. Brazilian president: US surveillance a 'breach of international law'. *The Guardian*. Retrieved from: https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance in 10/17/2019.
[63] Holland, S.; Hosenball, M.; Mason, J. 2014, January 17. 'Obama bans spying on leaders of U.S. allies, scales back NSA program'. *Reuters*. Retrieved from: https://www.reuters.com/article/us-usa-security-obama/obama-bans-spying-on-leaders-of-u-s-allies-scales-back-nsa-program-idUSBREA0G0JI20140117 in 10/17/2019.

subsequently reported that the agency stopped spying on friendly governments in Western Europe in response to the Edward Snowden revelations. Yet, the promise of the Directive cannot be really confirmed. [64]

Due to the impacts of international cooperation on individual rights (and to interstate diplomacy), the literature on accountability has suggested "old" and "new" mechanisms to control intelligence at this level.

In term of "old" mechanisms, Hayez (2011) argues that the cooperation would be better understood if the notion of intelligence and security services at the international level becomes more defined. Moreover, cooperation would be better controlled if it receives closer attention from every actor at the national accountability level. In this regard,

> The oversight of international intelligence cooperation has our dimensions. Firstly, it appears as a 'network of networks' of external relations (often called 'liaisons' in intelligence), which reaches up to several hundred foreign correspondents for a single intelligence or security service. The architecture of these liaisons is based on three pillars, each of them growing: a population of 'liaison officers' from the services deployed under diplomatic status in partner capitals, an agenda of bilateral meetings (between heads of services and between experts), and a thick web of electronic and secure channels of communications. Secondly, cooperation brings up an array of intelligence products, from raw data, flowing in almost real-time, to finished reports exchanged only after careful approval. These goods are disseminated in accordance with the level of intimacy of the bilateral relationship or the ad hoc purpose of the exchange. Thirdly, cooperation increases opportunities and methods, such as HUMINT (human intelligence) and SIGINT (signals intelligence). Cooperation helps to share the burden of an operation, in terms financial cost and political impacts (especially when operations fail, like several Anglo-US military actions in the Middle East). Fourthly, intelligence cooperation has a temporal dimension. It may take the form of a series of initiatives, prompted by emergencies and infrequently carried out by emergency circumstances to prevent an imminent threat (for example, a projected terrorist attack or cyberattacks). Rapid responses are common in counter-terrorism operations but also in other fields, such as counter-intelligence. Any oversight project should take into account that some intelligence operations are sometimes decided in urgent situations for ad hoc scenarios (Hayez, 2011, p. 166).

[64] Cole, D. 2013, October 29. 'We are all foreigners: NSA spying and the right of others'. *JustSecurity*. Retrieved from: https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/ in 10/18/2019. See also: *Amnesty International*, 2019 July 8. 'UK's surveillance powers to be considered by Europe's highest human rights court'. Retrieved from: https://www.amnesty.org/en/latest/news/2019/07/uk-surveillance-powers-to-be-considered-by-europes-highest-human-rights-court/ in 10/18/2019.

As Hayez mentions, the universe of intelligence cooperation has several formats, beyond the classical definition of informal/formal, and different temporalities. The complexity of the "network of networks" is an indicator of the rhizomatic characteristic of intelligence nowadays. From automated data exchange to human liaisons deployed in foreign countries, the definition of intelligence and its control are redefined to new levels of complexity and fluidity. Thus, for the sake of accountability and intelligence efficiency, countries must specify the conditions for the implementation of such cooperation in their laws. To do this, three models can be adopted: 1) to delegate authority, 2) to establish a community manager, 3) to operate by informal dialogue.

In the first model, as adopted in the Netherlands, the General Intelligence and Security Service (AIVD) and the Defense Intelligence and Security Service (DISS) establish a delegated authority to orient the international cooperation. According to Law 59 of February 7, 2002, the director of the Dutch intelligence and security service must authorize the provision of intelligence to a foreign partner. On the other hand, the minister of interior (AIVD) or the minister of defense (DISS) are the ones who authorize "technical and other forms of assistance" (i.e. participating in a joint operation) to foreign services.

The second model is to establish intelligence-community managers. This model is implemented in the United Kingdom, where the Joint Intelligence Committee (JIC) has the authority to maintain and supervise liaison with the Commonwealth and foreign intelligence organizations. This model is also implemented in Italy, where the "Dipartimento Delle Informazioni per la Sicurezza" (DIS), under the prime minister's authority, is empowered by the 3 August 2007 Act to have full knowledge of both Italian intelligence and security services' operations.

The third model is the informal dialogue between intelligence and security services, and the executive. This is the traditional way adopted by France, Spain, and even Brazil in the last century. Being informal does not mean that cooperation is illegal. Rather, it means that the supervision of the cooperation lacks a specialized, permanent and recognized channel. Yet, the new context has brought the need for explicit rules for international cooperation to facilitate the management and efficiency of intelligence. In this regard, national rules must establish a nodal point to coordinate international cooperation of intelligence and security services. Since 2002, the Director of the CNI has been required to supervise and coordinate actions of intelligence, something that includes tasks and information exchanged with foreign services. We will return to this point below. However, it is important to ensure the real capacity of internal audits and general inspections to evaluate the operations with foreign services. In internal terms, we cannot confirm if Spain and Brazil have independent control bodies to check the

proportionality, the efficiency, and the outcomes of international intelligence cooperation.

Another form to improve accountability in this domain is to reinforce external controls such as the role of Parliaments. In that sense, specialized commissions (such as the Spanish Commission of Reserved Funds and the Brazilian Commission for the Control of Intelligence Activities) should be given full jurisdiction to know and evaluate, both in a priori and a posteriori, the operations and forms related to international cooperation. In that sense, access to intelligence by the parliamentary bodies should be conducted in two conditions: respecting confidentiality or secrecy; and allowing full access to closed operations. Moreover, "the head of service should report at least once a year to the parliamentary commissions to clarify the international actions conducted under his/her supervision" (Hayez, 2011, p. 163). This formula might be essential to oversee new trends in intelligence, such as the use of subcontracts and the externalization of operations to private entities. Currently, those trends remain out of the radar of legislative and judicial controls. For instance, the Brazilian government has fostered public-private partnerships between the Ministry of Science, Technology, and Innovation (MCTI), banks and telecoms, and international research centers, to improve the responses of the government against cyberattacks.[65] We also mentioned the case in which the CNI and the Spanish National Police contracted the Italian company Hacking Team for operations in Spain and third countries (see section 3.4). This modus operandi can escape the oversight of external bodies, as in the case of financial crimes that remain absolved because business companies select the law of their choice to obtain a contract and evade responsibility. Therefore, changes in legislation are welcome to closely monitor international cooperation and avoid blurred responsibilities.

Changes in legislation are necessary if we consider that some Parliament bodies are prohibited to access any information related to international intelligence cooperation. In those cases, statutory provisions empower the Executive to deny access to information in accordance with specific criteria. In Spain, Article 11.2 of Law 11/2002 regulating the CNI denies the parliamentary access to "classified materials […] provided by foreign services and international organizations". This restriction aims to protect the secrecy and sensitive information from important foreign partners.

[65] However, when it comes time to truly articulate and implement PPPs in cyber defense, Latin American countries are confronted by the issue of "technological sovereignty" deficit (e.g., the capability and the autonomy to select, generate, acquire, and exploit commercial technology needed for cybersecurity defense). See: *Igarapé Institute*. 2014, December 1st. 'Deconstructing Cyber Security in Brazil: Threats and Responses'. Retrieved from: https://igarape.org.br/en/desconstruindo-a-seguranca-cibernetica-no-brasil-ameacas-e-respostas/ in 10/20/2019.

However, after the Snowden revelations of mass surveillance in 2013, the CNI Director was invoked to clarify whether the NSA or the CNI monitored electronic communications of Spanish citizens in domestic soil. In that time, the CNI Director declared that the service abides by legal rules and denied the revelations (see Section 3.5). If that explanation is correct, the communications of Spanish citizens were not intercepted by foreign intelligence agencies. However, the CNI cannot also confirm the opposite, the fact that an international partner with greater resources and technological capacity could have helped the CNI in antiterrorism and national security tasks by monitoring Spanish citizens. The denial of this kind of cooperation could have been claimed to keep trust and good relations with foreign services. In other words, attempts to sidestep national laws occur when states directly request foreign intelligence services to collect information on their behalf in order to bypass national regulations. In the 1990s, for example, there were allegations that the UK, USA, and Canada had used their joint ECHELON signals intelligence system to circumnavigate national laws on privacy and interception of communications (Campbell, 2000). These countries collaborated to spy on each other's citizens. In Spain, the NSA could have done the same during the last decade at the request (or by the omission) of Spanish authorities.

The hypothesis that the CNI used denial of responsibility is also supported by the fact that Spain depends on European and Anglo-Saxon partners to conduct operations. At the time of the Snowden revelation, documents proved the tight collaboration between the services in four levels of confidence.[66] Moreover, the idea of plausible denial might be pertinent because Spain has a strategic position, being one of the most important nodes to inform the situation regarding the Southern border of the European Union. For example, much of the literature describes the EU's policy in the Maghreb as driven by a quest for stability and a desire to maintain the status quo as a consequence of economic and energy interests on the domestic and international level (Eder, 2011). These motivations, articulated by their most persistent proponents (Spain, France, and Italy), had a great influence on the formulation of the EU's counter-terrorism policy towards North Africa. The Union has focused on a short-term status-quo oriented containment strategy, instead of tackling the root causes of the terrorist threat from across the Mediterranean. Such a strategy, in the eyes of the EU, reduces the threat levels to an acceptable level. At the same time, this strategy does not imperil the EU economic and energy interests in states such as Morocco, Algeria, Tunisia, and Libya. Consequently, democratization takes a backseat in the EU's relations with the Maghreb as the Union must be labeled "a realist actor in normative clothes. The frequently invoked image of Europe as a normative power is

[66] Aranda, G. 2013, October 30. 'El CNI facilitó el espionaje masivo de EEUU a España'. El Mundo. Retrieved from https://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html in 10/20/2019.

outdated" (Eder, 2011, p. 451). Therefore, there is no surprise if the CNI shows reluctance to disclose information regarding international partners in Europe and abroad.

In terms of foreign and security policy, and based on information given by the CNI website, Spain has focused on: a) sharing information about terrorist threats from the Maghreb and the Middle East, b) in collecting data about North Africa overall politics in order to analyze opportunities and to preserve the economic relations in a scenario of energetic competitiveness and social instability; and, c) the agency has worked in reports of intelligence to monitor irregular migration from those same areas. The latter point can be attested in the close relationship with the Moroccan government to assist in the refoulement of migrants in the Southern border. In that sense, the EU policies are only understood if international links in the Maghreb cooperate to make "the dirty work" to refrain terrorism and migration from North Africa (Cavatorta & Pace, 2010).

By creating an international blind spot to the accountability role of Parliament Commissions, countries like Spain seem to give more importance to international agreements than to national sovereignty. In that logic, it should be noted that the improvement of intelligence efficiency through foreign partner services cannot be achieved at the expense of the internal legitimacy of intelligence and security. "Even traditional partners have to understand that the proverbial third-party rule has to be rethought in a way compatible with the new national cadres" (Hayez, 2011, p. 161).

In the case of Brazil, the situation is normatively different but functionally similar. The Commission for the Control of Intelligence Activities (CCAI) has the capacity to oversee international cooperation. Article 10 from Resolution 3 from the National Congress of 2013 expresses that the CCAI has access to materials and pertinent information to the missions of ABIN that might be obtained from foreign services, respecting the classification of that information behind closed doors. This measure seems to be a response to the international surveillance executed by the NSA that same year. It became evident that Brazilian high officials and strategic companies, such as the Petrobras oil company, were monitored before becoming the epicenter of a corruption scandal (Lava Jato operation) that entailed institutional instability and political turmoil in Brazil and in neighbor countries. Yet, there are no public records or assessments regarding international cooperation. Congress initiatives to oversee this realm are also inexistent. If those actions existed, they had been produced in an informal base. In any case, they can evaluate the geopolitical position of Brazil as a hegemonic power in South America but as a very dependent country in terms of intelligence and technological counter-intelligence measures, especially from the global North. In the last years, the president Jair Bolsonaro, for example, has explicitly demonstrated the total alignment with American intelligence foreign policies, leaving ABIN and SISBIN as

underestimated tools to boost the Brazilian geopolitical potential and sovereignty.[67]

In other countries, the national oversight of intelligence international cooperation has also other problems. For example, Wright (Wright, 2011) had examined the contribution of ad hoc or special commissions to democratic oversight. Wright compares the role of those inquiries in Canada, Germany, and the United Kingdom. She affirms that they have provided a substantial degree of transparency in those countries. However, she also has detected significant challenges to their fact-finding and ameliorative mandates. That is, in attempting to shed light on international intelligence activities, domestic inquiries might not find essential information and conclusions. Paradoxically, they can create conditions to less transparency and accountability, and less public reassurance and confidence. This is because such inquiries did not avoid or diminish government brittleness about disclosure of classified information, including foreign-caveated information. Consequently, the inquiries did not avoid "tortuous", "time-consuming", "expensive" and therefore "potentially disaffecting results" (Wright, 2011, p. 188).

Notwithstanding, oversight bodies in states such as Norway, Belgium, Canada, the UK, and Australia review the activities of security services behind closed doors and issue public reports. This is something that could be created in Spain (to oversee international cooperation and to release public records or full documents with pen censorship in parts of the documents) and implemented and assessed in Brazil (to build public reports and *a posteriori* briefs that could serve to prospective measures in international cooperation). Such procedures are widely accepted as an appropriate compromise between accountability objectives and the need to protect security-sensitive information.

If domestic legislative bodies are still struggling to oversee international cooperation, another answer consists of creating provisional or permanent networks of accountability in this area. The principle is very simple: in order to tackle international issues, the response needs also to be formulated at the international level. In that sense, one of the recommendations is to create bilateral agreements between Parliament Commissions or accountability bodies. States could establish ad hoc or permanent agreements to comply with disclosure requests. In other words, two countries with established intelligence-sharing

[67] After the victory in the presidential election, Bolsonaro made a trip to the USA and visited Langley CIA Headquarters. The visit was a symbol of his alignment to American Policies. "No Brazilian president had ever paid a visit to the CIA," said Celso Amorim, who served as foreign minister under former President Luiz Inacio Lula da Silva and is a Bolsonaro critic. "This is an explicitly submissive position. Nothing compares to this." The CIA had no comment on the visit. From: Associated Press. 2019, March 18. 'Brazil's far-right president visits CIA on first U.S. trip'. *PBS*, News Hour. Retrieved from: https://www.pbs.org/newshour/world/brazils-far-right-president-visits-cia-on-first-u-s-trip in 10/23/2019.

relationships and comparable oversight frameworks could agree to disclose information to inquiries from the allied country. Another recommendation is to create joint international ad hoc inquiries. The idea of two states establishing ad hoc inquiries to review intelligence activities in which both countries were involved may seem dreamy. However, like Born, Leigh & Wills (2011) express, such a notion is not that far from internationally integrated ad hoc task forces and intelligence teams. Certainly, there would be issues of importance such as legislative frameworks, as well as institutional, partisan, and cultural differences. Yet, multilateral teams have to cope with those issues even in the realm of security. Intelligence operations and information sharing between states can be conducted despite the differences in those issues. In the same logic, accountability bodies might conclude that a supranational ad hoc inquiry should not be forestalled by such concerns.

> Ad hoc accountability networks could be novel creative and tailored solutions to adapt procedures, but also more conventional forms such as closed-door processes by a selected established record. They might mean solutions with elements of the new and the old, such as ad hoc cooperation with trustworthy foreign bodies. But the application of these solutions then begs a new paradoxical question of whether the essential character of domestic inquiries – particularly public inquiries – would be so fundamentally changed that they would look and feel simply like the investigations carried out by permanent oversight bodies (Born & Wills, 2011, p. 223).

The creation of new ad hoc inquiries to help permanent oversight bodies could provide countries with greater legitimacy and authority to hold states and their services to account. In the absence of such developments, serious doubts remain as to whether national parliamentary assemblies are appropriate institutions to undertake rigorous accountability roles.

In the case of Brazil, we have commented on the proposal to create a "technical body" to complement the role of the Parliament Commission (CCAI). Despite the proposal had no intention to oversee international cooperation, it could enhance a network of accountability that combines political boards (as in the case of the Commission) and technical expertise (Council) to improve the control of intelligence and counter-intelligence. It is known that security services are cautious when they disclose information according to the political moment and situation of the Houses, such as parliamentary groups and opposition parties that are not only interested in controlling this activity. Thus, a technical Council might compensate for the self-restraining logic adopted by intelligence when supplying accounts to external bodies. However, a technical body does not imply automatically in political neutrality nor a better assessment of secret services. This group can work as veto power or create blind spots for the strengthening of accountability actions, especially when they are indicated by the Executive power

itself. Nevertheless, deeper actions are welcome to improve the answerability and responses of the intelligence system either by old commissions or new bodies.

In the case of the European Union, new mechanisms to oversee international cooperation have emerged at continental level. The EU legislation can affect Member States (i.e., a regulation) when a Decision aims to unify "identical" rules across the Union, or when a Directive recommends harmonizing similar rules in different countries. Directives require to be implemented by national legislation that usually is approved by national Parliaments within two years. The result of this process is a patchwork of EU/national competences in many areas of law. However, because of the national security exceptionality, the oversight of intelligence services has barely been touched by the EU norms. Intelligence cooperation in the area of anti-terrorism continues to be a black box even when is linked to security and police cooperation. For example, the European police body (Europol) has no sufficient informational capacity and operational autonomy within the Union because it depends on the information and police intelligence from the Member States to tackle terrorism and organized crime (Busuioc & Groenleer, 2013). Despite that, Europol produces databases and crime assessments that are essential to monitor offenses and crime threats are checked by the European Data Protection Supervisor (EDPS) since 2017.[68]

In terms of international oversight, the European Parliament involves the Committee on Civil Liberties, Justice and Home Affairs (LIBE). The Committee is connected to national security, reporting, and adopting non-binding resolutions. At the same time, the European Court of Human Rights (ECHR) might judge decisions and establish legal lines to oversee the interference of fundamental right in the ground of national security. Those decisions are based on the European Convention of Human Rights that demand right to a fair trial (Article 6); to privacy, familiar life and inviolability of correspondence (Article 8); to freedom of expression (Article 10); and freedom of assembly and association (Article 11). Also, the European Court of Human Rights (ECHR) established by the Convention can tackle national security issues, such as in domestic courts judging limitations on the rights to liberty of movement, freedom to choose a residence within a state (Article 2(3)), and review a deportation decision (Article 1(2))). In that sense, the ECHR must assess and propose recommendations to balance the interests of individuals and the state.

In terms of intelligence and sensitive areas, the ECHR has traditionally adopted a stance of judicial restraint that permits states a leeway of interpretation. The ECHR justifies this timid role in the base of the "subsidiary nature of the protection enabled by the ECHR and the difficulty to identify common European

[68] European Data Protection Supervisor. 2016, May 19. 'New Regulation boosts the roles of EDPS and Europol'. Press release, retrieved from: https://edps.europa.eu/node/3336 in 12/01/2019.

concepts to the extent of rights and their restrictions" (not blue book, the new one, 2018: XX).

Hence, the ECHR has not acted as a classical intelligence accountability mechanism to directly refrain domestic intelligence that interfere fundamental rights. Instead, under the ECHR system, accountability is at the state level: the contracting states are responsible to comply with the ECHR. In that sense, the state is responsible when it fails to construct and implement satisfactory accountability mechanisms and institutions at the national level. For example, the European Court disallows the exercise of unrestricted intelligence powers that affect fundamental rights enacted by the ECHR. In that logic, Act of May 2002, which established the lines to authorize the CNI actions to suspend rights in Article 18 from the Spanish Constitution, was also motived on the jurisprudence formulated by the ECHR. That article rules the right to honor, to personal and family privacy and to personal image and needs to be in accordance with the ECHR jurisprudence such as Article 8 on the right to private and familiar life.

In addition, the Parliamentary Assembly of the Council of Europe (PACE), (not to be mistaken with the European Parliament) meets periodically to oversee security policies from member states. As the PACE is the parliamentary body of the Council, an entity that congregates 47 nations beyond the EU, it has not investigatory power to scrutinize secret actions as the traditional oversight bodies at the national level. The Assembly is a forum that discusses and adopts general resolutions and recommendations. At best, it can exert an influence on the Committee of Ministers. Yet, subsequent action in the area of intelligence and security by the Committee of Ministers is very unlikely.

Likewise the PACE, the "Venice Commission" is another advisory body of the Council of Europe. This is composed of independent experts in the field of constitutional law. The Venice Commission was created in 1990 for constitutional assistance in Central and Eastern European countries after the Cold War. The Commission's official name is the "European Commission for Democracy through Law" but it has received the name of the city where sessions take place four times a year. This Commission is not a fact-finding body (it lacks investigative powers). Rather, it performs as an advisory body on constitutional matters by independent experts appointed by their governments. The Venice Commission has looked at the CIA rendition flight program through constitutional and international law aspects. After that program, it has produced a detailed report on best practices in the field for the accountability of domestic security services.[69] The reports from the Venice Commission, alongside the reports from the Council of Europe Commissioner on

[69] *European Commission for Democracy through Law*. 2006, March 18. 'Opinion on the International legal obligations of Council of Europe member States in respect of secret detention facilities and inter-state transport of prisoners adopted by the Venice Commission at its 66th Plenary Session (17-18 March 2006)'. Retrieved from: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2006)009-e in 10/23/2019.

Human Rights –an independent body elected by the PACE-, provide recommendations to oversee operational aspects of security and intelligence in the European Union and beyond.[70]

Another example of an international oversight body was The European Parliament's Committee on Civil Liberties, Justice and Home Affairs, held in Brussels in 2015 by the Belgian House of Representatives' Committee, the German Bundestag's Parliamentary Oversight Panel and the Italian Parliament's Committee for the Security of the Republic. Those national committees joined as an inter-parliamentary committee to cope with the democratic oversight of intelligence services in the European Union. The Committee has examined issues such as the USA surveillance program, the impact on EU citizens' fundamental rights, and the transatlantic cooperation in Justice and Home Affairs. The meeting served to foster cooperation between national oversight bodies, allowing them to share best practices and to discuss common concerns. As in the case of the Venice Commission, the recommendations have not binding effect, although they can serve as complementary forms to improve the expertise and the roles of domestic Parliament Commissions. In that logic, supra-national (ad hoc or permanent) and domestic oversight bodies can constitute a prospective area in which representatives, technical advisors, and civil society organizations can work together to expand the accountability of intelligence and states.

A final example is the Court of Justice of the European Union (CJEU). It is the Chief judicial authority in the Union and oversees the harmonization of rules in Member States. In recent years, the CJEU has been developing jurisprudence on massive surveillance as certain states like the United Kingdom and France have established in their national legislation the obligation for providers of electronic communications services to transmit traffic and location data of users to a public authority or retain that data in a general or indiscriminate manner.

In October 2020, The CJEU has judged through a series of decisions (C-623/17, Privacy International, C-511/18, La Quadrature du Net and others, C-512/18, French Data Network and others, and C-520/18, Order of French-speaking and German-speaking lawyers from Belgium and others) that European Union law prevents national legislation from requiring an electronic communications provider to carry out the general and indiscriminate transmission or retention of traffic and location data for the purpose to safeguard national security and prevent crime. By those decisions, the CJEU recalls that the Directive on privacy and electronic communications is applicable even if the object of data processing is the safeguarding of national security. For this reason, a Member States may not restrict

[70] *European Commission for Democracy through Law*. 2015, December 15. 'On the democratic oversight of signals intelligence agencies'. 102nd Plenary Session. Retrieved from: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e in 10/24/2019.

the scope of the rights and obligations provided in the Directive on privacy and electronic communications. The CJEU, thus, emphasizes that the general and indiscriminate treatment of data constitutes a particularly serious infringement of the Charter of Fundamental Rights of the European Union.

In that sense, the CJEU concludes that, in cases of serious and foreseeable threats and damage, the Directive does not prevent the State from issuing an order in which service providers of electronic communications must keep, in a general and indiscriminate way, traffic and location data. However, this treatment must take place during a specific period of time, and the process must be reviewed by the courts or independent administrative bodies. In the case of Spain, it is not clear if indiscriminate and mass surveillance in the case of intelligence will be tackled by the traditional judicial control or by a Data Protection Authority. Nevertheless, this means that a new front has been opened by third dimension accountability entities. This front, in turn, is connected with domestic data protection rules (See Chapter 5 section 5.1).

Epilogue

To vertical and horizontal accountability, we can add the third dimension as a mechanism comprised of international actors and organizations. The greatest issue to the effectiveness of third dimension actors to oversee state security and intelligence agencies is the sovereignty of the state. The sovereign power of states makes them ignore pressures from abroad in many circumstances. Nevertheless, as the world becomes more interconnected, pressure over states can be exercised when external actors control access to resources or status, or when states depend on other countries to conduct policies and share information.

This section has shown the multiplicity of actors and mechanisms involved in accountability at the international level. It suggests that one should avoid focusing narrowly on legislation and other formal powers surrounding intelligence services, and pay greater attention to the wider environment of actual and potential accountability mechanisms. While the legal framework is important due to its role in establishing the official mandate of a security intelligence agency and the relationships with other key institutions, legislation should be complemented with international mechanisms that redefine the access to restricted information and the suspension of fundamental rights. For Lustgarten (2004), rather than legislation, it is the internalization of political values (like coordination and transparency) within the political culture, especially among the political elite, that provides "the most essential indicator of legitimate governance of the security sphere" (Lustgarten, 2004, p. 14).

In this section, we have shown that the principle of "plausible denial" is useful to shield intelligence procedures, such as covert actions and secret information. Plausible denial is the doctrine that 'even if a state's involvement in covert action becomes known, the chief of the polity should be able to deny that he/she authorized or even knew the action. The decision-maker should be able to assert, with some plausibility, that it was carried out by subordinates "who acted without his/her knowledge or authority" (Shulsky & Schmitt, 2002, p. 92). However, plausible denial corrodes the principle of accountability and insulates top decision-makers and political authorities from the consequences of intelligence operations that may "prove controversial if brought to light" (Caparini, 2016, p. 18). Moreover, security intelligence agencies may prefer to inform Ministers minimally in order to preserve their "capacity for plausible denial when an operation fails and prove embarrassing or controversial" (Gill in Caparini, 2016, p. 18). In that sense, regulations as well as a sense of responsibility should be enhanced to avoid plausible denial proliferation. An intelligence operation, for example, should be directly assigned to public officials by clear lines, legal mandates, warrants, and awareness in order to recognize (shared) responsibilities, impacts, and consequences.

In addition, control and oversight of intelligence are challenged by the issue of national security. Under international law, states can legitimately limit certain basic rights on the grounds of clear danger or immediate threat to national security. However, countries have used allegations of domestic terrorism to allow their police and intelligence agencies to torture citizens whom they perceive to be a threat to a regime or to the government itself. Yet, it is difficult to assess to what extent a state which is not involved in such practices is permitted by international law to receive and make use of intelligence and information that came (or has reason to suspect that came) from torture or other violation on human and constitutional rights. This dilemma, then, consists of turning accountable a state or a domestic organization, which has been involved, aided or assisted a rendition, arbitrary detention, torture, and ill-treatment of an individual, in order to assume its international responsibility for those particular acts. Moreover, states that receive information based on arbitrary violations of fundamental rights should also share responsibility by those acts. That responsibility should be accounted to domestic bodies such as Legislative and Judicial power. For example, networks of cooperation, as the past Condor Operation between the military regimes in South America to surveille dissidents and commit political crimes (see section 2), are one reason that stands for the importance of overseeing the share of strategic information between states. The inexistence of international accountability networks endangers the very existence of accountability and increases the opportunity to plausible denial and illegitimate actions conducted across states.

In that sense, we expressed that the Spanish government and the CNI probably used the argument of plausible deniability of responsibility in the

collaboration with the so-called rendition flights of the CIA since 2002. In doing so, they used a tactic that inhibits greater levels of accountability, such as answerability and enforcement, to learn from past mistakes and improve international cooperation with international services. This effort is challenging if we consider that the CNI regulation does not allow Parliament Commissions to access and analyze international cooperation. That restriction preserves an uncovered legal zone where is possible to perform plausible denial and mask deviations of power alongside international players. In the case of Brazil, the regulation of ABIN allows the Parliamentary control to oversee international cooperation. However, there are neither public records nor assessments of ABIN actions regarding international links and operations.

In that sense, the Spanish Committee of Reserved Funds and the Brazilian Committee for the Control of Intelligence Activities should improve the jurisdiction and expertise to assess the cooperation of the services with their foreign partners. The access to that cooperation might be allowed on two conditions: the confidentiality of the access must be effectively enforced, and the oversight should be allowed especially for closed operations. Hayez (2011) supports that the head of the service must report international cooperation activities to the parliamentary overseer at least once a year. In that sense, oversight bodies might review the activities of security services behind closed doors and then issue basic public reports.

Moreover, Spain and Brazil should reformulate their procedures to handle and process classified information. To solve the delicate balance between confidentiality and accountability, this dilemma could be managed through the principle of deferred transparency. That is, by the declassification of confidential material after a period prescribed by law. We believe this principle should be created in Spain and implemented in Brazil, in order to tailor national legislation to disclose historical archives and to release public reports to assess the work of legislative commissions, the judicial control of intelligence, and the internal control of the Executive.

In that sense, the reports should be delivered in two velocities: one related to the past and other to the present. The first one consists of reports regarding closed operations and outcomes of intelligence (submitted to renewed laws of declassification, historical memory, and access to information). These reports might be released under the criteria of pen-censorship to avoid conflicts against personal data protection, privacy safeguards, and fundamental rights. The second one relates to reports released by the controls performed by the three powers of the state (see previous sections). Indeed, some of the bodies release more information than other ones, as in the case of the legislative. Nevertheless, those branches should release data beyond their regular formalities and tasks (i.e. the National Intelligence Policy or Directives released by the Executive). Thus, the

powers of the state should release overall reports expressing current statistics, policy goals, concrete measures, expected outcomes, and as much information that can be published (without compromising names, sources, operations, and justified national security matters). Those reports should contain, at the same time, evaluation of previous reports and intelligence actions. That is, the reports should evaluate or make a substantial assessment of both retrospective and current policies, beyond technical and descriptive information.

The idea is that, besides the huge amounts of technical data produced every day by the administration, there must be overall reports to address every citizen in the country, so they can understand and endorse the role both from intelligence and from the controllers of intelligence. The roles and reports should not coincide and necessarily support each other, as a certain distance and critical position are essential to the assessment between the powers of the state. Yet, they should converge to enact a broad *community of intelligence and accountability*, as a further step to legitimize the relationship between the state and citizens. Foreign competitors would barely benefit from those reports insofar they preserve key information, showing general plans and policies that are normally known and undertaken by other states.

Furthermore, we mentioned innovative mechanisms of accountability such as the creation of new inquiry bodies to the aid of traditional accountability measures. In that sense, establishing ad hoc or permanent oversight bodies could provide countries with greater legitimacy and authority to hold states and their services to account. In the absence of such developments, serious doubts remain as to whether national parliamentary assemblies are appropriate institutions to undertake rigorous investigative work. International actors such as the Venice Commission and the European Parliament's Committee on Civil Liberties had recommended adopting the principle of deferred transparency as explained above. In parallel, different bodies of accountability across the administration (beyond intelligence and security policies) should create a sphere of participation, plurality, and deeper reform considering citizens beyond the mere role of consumers of norms and receivers of protection by the state. We hope that a sphere of accountability and ethics emerge as a professional niche and as a new form of doing politics in the public administration in the future, going beyond the first wave of transparency in the last decades that aimed to redefine managerial rules to create laws to access information. As supported in this study, the aim of accountability should go beyond the aim to improve transparency and the attempt to restrain authority. Accountability should be replenished to enlarge legitimacy. We will revisit the concept of accountability in the final Part 4.

So far, we have expressed the main aspects of accountability in the third dimension. Those aspects are represented in Table 12. At this point, what are the

overall accountability mechanisms and principles enhanced by the third dimension?

In Spain, the CNI and the intelligence community are indirectly accountable to the International Law, such as the Convention Against Torture (CAT), to European regulations, such as the Charter of Fundamental Rights of the European Union, The Court of Justice of the European Union (CJEU), and European Forums, as the Venice Commission and The European Parliament's Committee on Civil Liberties. Intelligence services could be demanded, via classical forms of horizontal and vertical accountability, to fulfill international treaties and regulations. Eventually, they should justify and clarify their participation or assistance in actions against the International Law and fundamental rights established in the Constitution. This was the case of the CIA rendition flights conducted in Spain, which demanded a series of initiatives by the Parliament to clarify those operations. Another example is the Snowden revelations of international mass surveillance that affected citizens in several countries, including Spain. However, the domestic accountability mechanisms in Spain do not allow to address the forms of international cooperation, to control covert actions in international soil, to verify the exchange of information in military operations, and to assess the contracting of international companies and third organizations that assist the Spanish intelligence. In those domains, several forms to strengthen classical forms of horizontal and vertical accountability can still be developed alongside new oversight bodies at European and international levels.

In Brazil, the ABIN and the SISBIN are indirectly accountable to International Law and continental regulations, such as the foundational principles of the Organization of American States (OAS) and the guidelines of the Mercosur. Yet, the latter examples are not considered as international regulations or real forums of discussion for security and intelligence. The intelligence services could be demanded, via classical forms of horizontal and vertical accountability, to fulfill international treaties and regulations; and –contrary to the Spanish case- to verify the effectiveness and the forms of international cooperation via the legislative power. However, this kind of supervision has not been executed by the legislative commissions during the last years, and the control is not sufficient to oversee covert actions conducted in international soil (regardless the assistance in military and foreign humanitarian missions), and the contracting of international companies. In terms of international contracting, this point is partially addressed by internal controls and audits and by the role of media and civil society (topics in the next section).

Table 12: Accountability in the third dimension.

Accountability dimensions	Cases	
	Spain	Brazil
Who is accountable?	National Intelligence Agency (CNI) and the intelligence community	Brazilian Intelligence Agency (ABIN) as coordinator of SISBIN
To whom are they accountable?	Indirectly, to International Law, European regulations, and European Forums	Indirectly, to International Law
About what are the services accountable?	More addressed: - *The fulfillment of international rules* Not addressed: - *The effectiveness and forms of international cooperation* - *Covert actions in international soil* - *The contracting of international companies and third players*	More addressed: - *The fulfillment of international rules* - *The effectiveness and forms of international cooperation* Less addressed: - *Covert actions in international soil* - *The contracting of international companies and third players*
How are they accountable? (measures)	Eventually, justifying and clarifying participation or assistance in violations against the International Law or fundamental rights with/by international players. For harmonizing domestic rules on intelligence and data with European jurisdiction.	Eventually, demanding the main ways of international cooperation via legislative control, or by pressure of media and international leaks.
Assessing accountability according to its internal principles	Did the accountability action result or promote at least one of the following principles? -Answerability ~~-Responsibility~~ ~~-Enforcement (punishment)~~ ~~-Transparency~~	Did the accountability action result or promote at least one of the following principles? -Answerability ~~-Responsibility~~ ~~-Enforcement (punishment)~~ ~~-Transparency~~

Source: author

The performance of public accountability as a connector between authority and legitimacy is a question of interest even in the accountability of the third dimension. When authority is called to give an account, if that action does not entail more legitimacy, then accountability fails to reach its objective. In that logic, when an authority from intelligence is called to be accountable by the third dimension, it is possible to speak of accountability especially (if not only) by answerability. That is, the international level copes with the sovereign capacity of the state to establish their own rules to intelligence. However, actors from the international level have influence and redefine the capacity to cooperate and formulate intelligence in domestic issues, especially in a complex and interdependent world. The international level can demand justifications, explanations, corrections, and even modifications in the legislation of the

countries, especially to overcome plausible denial excuses and enact the role of legislative bodies and domestic courts.

Despite the potential to redefine other forms of accountability, the third dimension is still being ignored by most governments as an opportunity to strengthen traditional forms of accountability. If responsibility is a value that can be promoted by new institutional and legal reforms to oversee international cooperation, other values like enforcement and transparency are left behind because the International Law has no binding effects on matters of national security, or because the global sphere is still understood as the "anarchic" order of competition between states. Yet, even the most hostile scenario for trust and rules demands basic codes of cooperation, sharing of standards, and commitment to protecting people. To change this scenario, international courts such as the CJEU have started to take decision on mass surveillance and data protection rules even in national security domains. And European countries have also thought in implementing a common intelligence body although this issue remains opened. Moreover, in this dimension, it is said that ethics appears as a solution to many of the international dilemmas of accountability. Intelligence agencies and practitioners know this, as codes of trust, cooperation, and links with foreign partners are essential to execute tasks and orient policies in the "international anarchic order". In the end, the international level is far from being an untamed territory with no rules, and cooperation might be fostered with competitor states and organizations, and also to construct international accountability networks.

In that effort, not only the role of intelligence practitioners is important, but also the role of media and civil society to synchronize legitimacy and authority as well as ethics and praxis. When those dimensions are dissonant or clash, even practitioners have challenged their organizations blowing the whistle. If the international level brings new challenges to accountability, now we address the folds and interstices of civil society.

3.8. The media role and civil society

We have shown that intelligence services in our cases are submitted to institutional forms of control. However, what is the role of the media and civil society to oversee intelligence? If this activity aims to protect the national security and the rest of society, how this arena relates to the protection of freedom of speech, opinion, assembly, political opposition, political protest, and legitimate dissidence? Can those groups reformulate the accountability mechanisms of intelligence? Let us answer these questions by considering the role of the media, scholars, whistleblowers, WikiLeaks, and novelists. This mosaic of roles allows to cover many possibilities and limitations from the public when it comes to foster accountability.

3.8.a. The media role and scholars

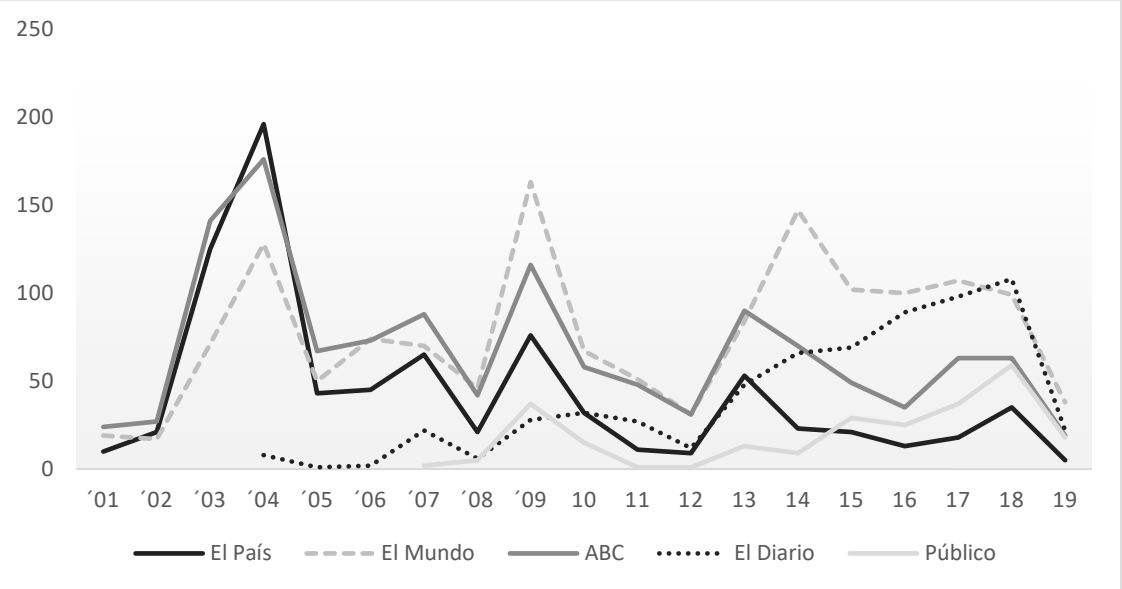
One of the most appreciated qualities to extend the base of the legitimacy of governments is to develop and strengthen a robust "civil society" with the capacity to influence policies, monitor government, and resist to authoritarian trends. In that sense, the media not only has a prescription role of showing news and reporting facts but also to create substantial coverage that can help to connect public audience and policies. In that sense, Florina Matei identified five points of importance for the media: 1) to inform the general public; 2) to connect government with the citizens; 3) to boost government legitimacy; 4) to exercises informal external oversight of the government; 5) to provide a ''learning'' environment for elected officials and the public. In the next pages, we analyze these points (Matei, 2014, p. 74).

In the first point, to inform the public, the media is defined as the array of communicative agencies (public or private) whose basic function is to inform the citizenry and shape public opinion. Few citizens have the time and resources to do their own research on politics and government policies, including elections, national security, and international developments. They use to rely on the media to acquire information, knowledge, and form ideas.

According to Matei (2014, p. 78), "the media observe, report, and channel important political and security information to the public, and help the public interpret information and form opinions, thus, fostering citizens' participation in political life". In terms of intelligence, the media inform citizens on security issues—from threats and challenges to national security, to current government policies, tasks, and missions of intelligence services as well as from police and the military. The media can also release information about the wrongdoing and failures of security institutions, including in a retrospective manner or years later. For example, in Spain, the media coverage of intelligence wrongdoing and scandals

in the 1990s allowed the citizens to know for the first time in history the existence of secret services. As Díaz-Fernández notes: "After years in which the intelligence services were inexistent for the citizens, they suddenly were surprised with the outbreak of a new period where the Spaniards daily had breakfast reading news about undercover activities of the intelligence services" (Díaz-Fernández, in Matei, 2014, p. 79).

Figure 11: Media coverage of intelligence in Spain



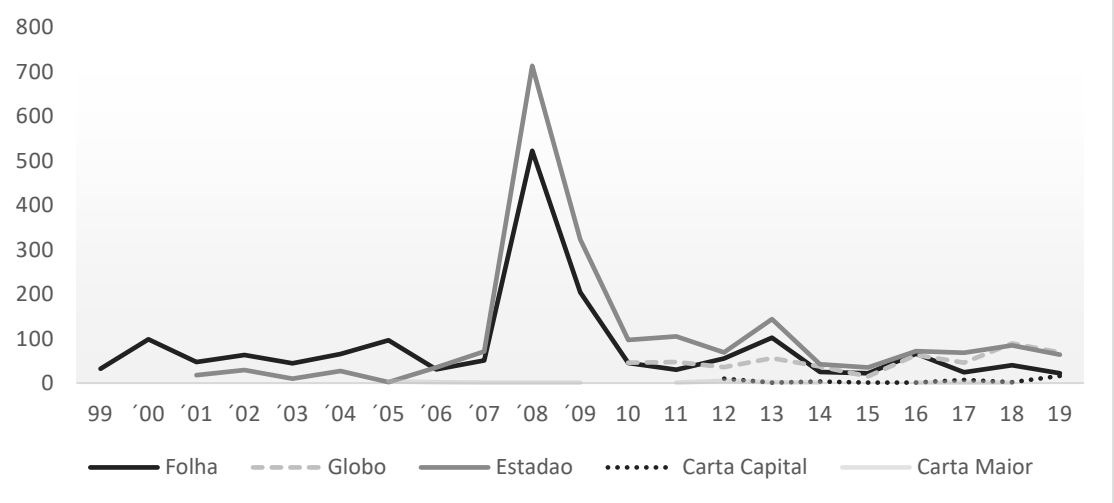
Soure: author

In the Spanish case, the figure above shows the media coverage of intelligence in the last institutional cycle or reform of the intelligence community (from 2001 to July 2019). The vertical axis exhibits the number of articles released by five of the major newspapers in the country. To build the graphic, we have selected those articles that tagged the "CNI" (Centro Nacional de Inteligencia) at least once. Thus, not all the articles have the CNI as their main object or analyze the Center (See Annex III in Appendices). Nevertheless, the time series in the early years depicts a scenario dominated by traditional media like *El País*, *ABC,* and *El Mundo*. It is possible to recognize a coverage peak in 2004 as the Madrid bombings by Al Qaeda opened a huge discussion about the role of the intelligence community and the efficiency of CNI. In the following years, the articles covered issues like the CIA rendition flights and the War in Afghanistan and Iraq. In 2009, another peak (169 articles by *El Mundo*, the same newspaper that released the CESID papers in the 90s, and 116 articles by *ABC*) is produced by cases such as the internal crisis of the CNI that caused the replacement of director Alberto Saiz by Sanz Roldán, who commanded the Center until 2019. That same year, *El Mundo* focused on cases like "Alakrana" (involving Somalian pirates and the Spanish navy) and antiterrorism actions in Spain. In the next years, *El Mundo* has echoed the official narratives and supported the Center in many occasions, such as in the effort against the group

ETA. Since 2012, it is important to notice that recent newspapers, sometimes more critical to official narratives, have occupied considerable space in the media. Independent leftwing newspapers like *El Diario* and *Publico*, despite the late reaction, developed a consistent number of publications (more than 50 articles per year). These newspapers have focused on issues such as the Snowden revelations, the control of Reserved Funds, the legislative commissions to oversee Defense, scandals of corruption and prevarication in the Ministry of Interior (*Cloacas de Interior*), and so on. In the last two years, the issues that were covered by almost all the media included the corruption cases *Villarejo* (criminal organization, bribery and money laundering in the National Police) and *Pequeño Nicolás* (forgery, fraud and identity theft of a fake CNI agent) the *WannaCry* cyberattack that affected multinational companies, and the Barcelona terrorist attacks repercussion in 2018.

In turn, in the Brazilian case, figure 12 shows the media coverage of intelligence in the last institutional cycle or reform of the intelligence community (from 1999, year of creation of ABIN, to July 2019). The vertical axis exhibits the number of articles released by five of the major newspapers in the country. To build the graphic, we have selected those articles that tagged "ABIN" (Agência Brasileira de Inteligência) at least once. Thus, not all the articles have the ABIN as their main object (See Annex IV in Appendices). Yet, the time series in this country shows a constant volume of publications that orbits 100 (one hundred) articles released each year, which demonstrates an amount of information about intelligence comparable to the coverage of the Spanish newspapers. As in the case of Spain, traditional newspapers like *Folha*, *Estadao*, and *Globo* (*O Globo* became *G1* since 2009) dominate the series. Independent leftist newspapers like *Carta Capital* (since 2012) and *Carta Maior* (since 2009) had an inexpressive volume of publications or did not address intelligence in their publications.

Figure 12: Media coverage of intelligence in Brazil



Source: author

In the first years in the figure above, the press covers topics such as the memory of the dictatorship, terrorist attacks in third countries, and foreign intelligence and diplomacy. It is interesting to note the huge leap of articles released in 2008 (713 articles by *Estadao*, and 522 by *Folha*) as a consequence of the espionage on the Supreme Court, and the political turmoil caused by the collusion between the Federal Police and the ABIN in the *Satiagraha Operation*. This case can be considered as the "Brazilian Watergate" in terms of illegal investigation from intelligence and police agents to prosecute money laundering and financial crimes. In this case, the media coverage caused the dismissal of the Directors in both of the security agencies. After this year, the media focused on cases of alleged infiltration of foreign terrorists in Brazil, the massive protests in 2013, and the preparation and security of the Olympic Games in 2016. This explains two minor peaks in terms of articles released in those years. More recently, traditional newspapers have focused on topics related to fake news and leaks, as in the case of fake news during the last presidential campaign and the revelations of the *Intercept Brazil* echoed by other newspapers in the case *VazaJato* (in which the major anticorruption operation, *Lava Jato*, was secretly conducted by the collusion between judges and prosecutors to enforce politicians and businessmen).

In the second point, regarding liaising government with citizens, the media, and other groups of civil society are channels that could enhance certain levels of transparency in a space of secrecy. If media contributes to the debate, communicating security institutions with policymakers, and with the citizenry, these connections could create spaces of feedback where the media can shape both public and government agendas. In Brazil, in 2005, the Brazilian Intelligence Agency (ABIN) invited journalists to the first conference on "Intelligence and Democracy", whereby the Agency expressed the need for intelligence in a democratic system, and the need to balance transparency and efficiency. However, media can also leak information that public officials or intelligence services do not want to be released. In other cases, media acts as a mechanism of transmission of classified information that internal practitioners release to journalists as parliaments and courts are reluctant to receive sensitive information by unofficial channels. In that sense, media contributes to dodge rules of declassification. As examples, in Brazil, in 2005, information was leaked to the media regarding the Satiagraha Operation, which involved illegal wiretapping by the Federal Police and the ABIN to monitor politicians, ministers, bankers, public servants, lawyers, and judges. In Spain, in 1995, Juan Alberto Perote, leader of the Operations Group attached to the "Centro Superior de Informacion de la Defensa" (CESID), leaked 1200 documents from the intelligence service. The Perote leaks revealed illegal wiretapping by the intelligence services of politicians, journalists, and other public figures, including King Juan Carlos. In this case, the media also revealed the plans

to create death squads that killed 27 people from 1983–1987 during the "dirty war" against the armed Basque separatist group ETA (Díaz-Fernández, 2010).

At the same time, the media can be aligned to certain political preferences and parties in order to be a channel of dialogue between government (and intelligence services) and citizens. Opposition parties may also use the media to raise citizens' interest in a particular topic or to appoint government misconduct. In Spain, for example, there is a highly politicized press compared to Brazil. In the first decade of this century, "Television, radio, and newspapers at national, regional, and local levels are generally aligned with a political party, and this is frequently reflected in their news content, as well as on their editorial pages" (Schweid, in Matei, 2014, p. 79). Partiality in the media´s role is expected, but only until a certain point. Intelligence services are part of governments, and whereas government legitimacy stems from the people, their pluralistic and heterogeneous interests actually symbolize the national interest, even if those opinions appear segmented and disaggregated. In simple words, people's voices should be heard, and the media is one of the places to do so.

In the third point, the media can help to boost government legitimacy. This is a crucial point to our study since we are interested in expanding the sources of legitimacy that sustain (or are connected) with forms of authority. Through the media, intelligence agencies can obtain trust and support from elites and the public even if they work in secrecy. The media is an important space for public access to intelligence legislation, structures, personnel, reforms, declassified data, and overall subjects. In Spain and Brazil, intelligence agencies have Websites where the public can obtain general information regarding their roles and missions, as well as about the mechanisms of civilian control from the Legislative power. In the case of Spain, by sponsoring professional and scholar formation of intelligence analysts in Madrid, the CNI, for example, seeks to expand the base of professionals and boost its legitimacy reaching academia, think-tanks, the media, and eventually the public.[71]

From the intelligence perspective, this approach may consolidate public trust, whereas citizens will appreciate intelligence efforts to become more open. However, this effort should be continuous and not only related to the pragmatic necessities of the intelligence community. It would be valuable if intelligence, both in Spain and Brazil, calls the media and other groups of civil society to discuss structural reforms of intelligence. For instance, those groups can be consulted to discuss the intelligence directives presented by the government every year, showing to citizens that the agencies work according to the legal framework and mandates imposed upon them by elected policy-makers but also by considering the interest of the public. To formulate policies, he "people", the main source of

[71] See intelligence culture and CNI partnerships with civil society in: https://www.cni.es/es/culturainteligencia/convenios/, consulted in 10/29/2019.

legitimacy, tend to be distant or not directly considered by bureaucracies. However, people offer deeper and stronger bases of legitimacy if compared to the direct but lesser legitimacy mediated by policy-makers. This idea redefines the relationship between agents and principals discussed in previous forms of accountability (see Chapter 1). In that sense, the inclusion of a wide spectrum of groups, opinions, and perspectives in debates on the formulations, implementation, and evaluation of intelligence and national security policies might result in the improvement of legitimacy within the intelligence realm. The problem, then, hinges on citizens' access to secrecy and classified information. We return to this tension in the last part of this study.

In the fourth point, the media can be deemed as an informal external mechanism to oversee the government. This means acting as a "watchdog" against government wrongdoing and abuse of power and exposing government transgressions to domestic and international audiences. In that logic, the media might foster public scrutiny and demand prompting responses from the government.

> As Britain's Lord Macaulay stated as early as 1832, media is a ''fourth estate'' because it complements the three official branches of government—the executive, legislative, and judiciary—if or when these are unable or unwilling to fulfill their responsibilities. In this context, American journalist Peter Eisner noted that "journalism . . . has always had a basic obligation—standing up to power and reporting to the public on the abuse of power, as a sort of ombudsman." Or, as Claudia Hillebrand asserted, media has "an obligation to keep governments in check and investigate their activities. This includes the realm of intelligence." To paraphrase United States military officer Jon Mordan, who addressed the relationship between the military and the media in a democracy, essentially, the news media are suspicious of the intelligence sector. And they should be. Questioning is the media's job because intelligence without public scrutiny can lead to dictatorship. And a return to dictatorship is what new democracies admittedly and hopefully want to avoid (Matei, 2014, p. 86).

In that sense, media could spark different forms of accountability such as answerability and enforcement, as in the case when justice courts react to media reports on alleged crimes or illegal actions that unmask governments illegitimate actions. In the previous sections, we have seen how the Parliamentary Commission for Reserved Credits and Spain and the Congress Commission for the Control of Intelligence Activities in Brazil used several times information from newspapers and the media to demand justifications and explanations from the Executive. For example, in the case of the CIA rendition flights, in the use of credits for personal benefit (as in the case *Corinna*), in the creation of liaisons to conduct parallel and illegal investigations (case *Villarejo*), or in the events of the *Satiagraha Operation*,

and alleged collusion between Brazilian Land Movements and the Venezuelan government, all those cases were firstly released in national newspapers or magazines. Yet, the information conveyed in some cases was not true, and each media had its political position and limitation. All the same, they might act like catalyst mechanisms to activate reactions by legislators that in turn produce deeper accountable actions. In addition, some of the media stories could be partial or incomplete as they do not necessarily address the oversight art of the government. This is because the informal oversight carried out by the media might be developed through the lens of scandal, such as the exposure of human rights abuses, misappropriation of funds, or other violations that might force other formal accountability mechanisms to do their job more effectively, such as to start investigations and even change legislation.

In our cases, and despite concerns about the objectivity of the press, the Brazilian media has exposed, since the 1990s, reforms, and failures, as well as abuses and wrongdoing in intelligence. For example, in 1992, the Brazilian press was the first channel to investigate allegations of corruption and abuse of power against President Fernando Collor. The first "Brazilian Watergate" eventually led to his impeachment by the Congress in that year. Also notable was the exposure by the media of the Satiagraha Operation, which resulted in hearings before the Congress, and the removal of the ABIN and Federal Police directors (Gonçalves, 2010). In Spain, the mentioned CESID papers resulted in the removal of the Socialist Deputy Prime Minister, Narcis Serra, the Defense Minister, Garcia Vargas, and the CESID director, Emilio Manglano.[72] More recently, also in Spain, the 2009 allegations by El Mundo about the CNI Director Alberto Saiz's misappropriation of public funds, nepotism, and other abuses eventually led the President José Luis Zapatero to ask Saiz resignation (Díaz-Fernández, 2010).

Those examples were produced by the press investigative function, in which a journalist or groups of journalists search for possible wrongdoing, law-breaking, or abuse of power within government and other institutions. This informal accountability mechanism is explained because the internal control usually does not check the inappropriate behavior of bureaucrats. Thus, when formal external controllers do not identify and challenge the government, the potential for insiders and journalists to leak information or investigate and report misconducts and suspects actions (sometimes not that suspect) draw attention from the public.

In order to collect a story, the media can use intelligence and national security agencies as potential objects and suppliers. At the same time, those

[72] Lazaroff, L. 1997, July 10. 'Spain's former covert operations chief sentenced to seven years'. *AP News*. Archive. Retrieved from: http://www.apnewsarchive.com/1997/Spain-s-former-covert-operations-chief-sentenced-to-seven-years/id-cbafdbd43779865fa7ed0f6aeb7f3a01 in 11/01/2019.

agencies can see the media as a possible partner to legitimate their actions or as actors with the capacity to undermine intelligence reputation if they "sniffle" around to disclose secrets. Under these circumstances, a mutual lack of trust is expected between the media and intelligence. In extreme circumstances, according to the perspective of intelligence, "reporters don't understand the need for withholding some information; the media can interfere with ongoing operations; […] reporters are always digging for dirt; the media sensationalize stories" (Matei, 2014, p. 86). Thus, intelligence and the media might collide against each other, but they also have a symbiotic relationship

In the fifth point expressed by Matei (2014), the media can provide a learning environment for elected officials and the public. According to her, to be "effective overseers", elected officials, particularly lawmakers, need to increase their interest in intelligence issues and create awareness about the importance of security institutions. The media (and other civil society actors, such as non-governmental organizations, academia, and interest groups) can be suitable vehicles toward these ends. This explains, in part, why intelligence agencies had created official publications, with partnerships or contributions from scholars, in order to build stronger relations with civil society. Not only this helps to increase the legitimacy of intelligence services, but it also promotes an environment where practitioners, bureaucrats, and academics interact to share specific knowledge that can be used to improve the efficiency of intelligence and the professionalization of this activity.

Table 13 below shows the number of academic articles released by the main intelligence Journals/Magazines in Spain and Brazil. In Spain, publications of scholars and practitioners are released especially in *Inteligencia y Seguridad* (2006-2016) transformed into the *International Journal of Intelligence, Security, and Public Affairs* (since 2016). The Journal began as the first Spanish scientific journal dedicated to the study of intelligence. According to the official website, "its main goal is to investigate and study intelligence for decision making in a broad sense. It is a meeting point for professionals and academics where they tackle rigorously a wide range of subjects in this field, including issues related to the practice of intelligence in democratic societies". In Brazil, the interaction between intelligence practitioners and academics is coordinated by the ABIN itself in a series of papers released annually by "Cadernos da ABIN", transformed into *The Brazilian Journal of Intelligence* (RBI) in 2009. This is an annual publication of the School of Intelligence (ESINT) from the Brazilian Intelligence Agency (ABIN). According to the official website, the RBI seeks to "promote the study, debate, and reflection on current issues related to the activity and discipline of Intelligence. The RBI accepts the participation of academic and professional authors, whose works deal with theoretical and practical issues of Intelligence, from the perspective of applied social sciences, humanities, natural sciences, and technology".

Table 13: Academic coverage of accountability in intelligence journals

	Spain		Brazil	
Year	Inteligencia y Seguridad (2006 -2016) Intelligence, Security, and Public Affairs (2016 - 2019)		Cadernos da ABIN (2005 - 2007) The Brazilian Journal of Intelligence (2009-2019)	
	Number of articles (total)	Subjects	Number of articles (total)	Subjects
2005	--	--	2 (9)	External control, Ethics
2006	0 (6)	--	2 (19)	Democracy and intelligence, Professionalization
2007	3 (12)	Legislation, Intelligence and academics in Iberoamerica, official secrets, and transparency	0 (13)	--
2008	2 (14)	External control (Peru), Judicial control and official secrets	--	--
2009	0 (18)	--	1 (9)	Intelligence and users
2010	2 (8)	Legislation (competitive intelligence), Legislation (Ukraine)	--	--
2011	1 (12)	Legislation (Germany)	2 (10)	Democracy and intelligence, Legislation (general)
2012	5 (19)	Democracy and intelligence (Latin America), Legislation (Italy), External control (CNI economics), Official secrets and Criminal Law, Parliamentary control	0 (10)	--
2013	0 (16)	--	1 (10)	Legislation (Information access)
2014	2 (11)	Judicial control (CNI), Parliamentary control	--	--
2015	--	--	1 (7)	Legislation (Privacy)
2016	1 (17)	Ethics (Snowden revelations)	1 (6)	External control (financial control of ABIN)
2017	1 (11)	Legislation (Australia)	2 (8)	Legislation (Information access and official secrets), Ethics (Human security)
2018	2 (11)	Legislation (Costa Rica), Official secrets and external control (Poland)	1 (9)	Legislation (Law proposals and Bills)
2019	1 (6)	Legislation and external control (United States)	--	--
Total	20 (161)		13 (110)	
Total (%)	12,4 %		11,8 %	

Source: author

The table above shows the number of articles released each year and the subjects covered by the journals. From our point of interest, the topics that can contribute to accountability and legitimacy of intelligence were separated from the overall production (number in parenthesis). In light of that, the topics addressed in the history of the journals that can be linked with our study are legislation and institutional design, external controls, ethics, democracy and intelligence, and official secrets. Those categories are specified in each year and country as seen above. Yet, considering the amplitude and importance of these topics, the percentage of academic and professional articles in the journals regards only to 12,4% (Spain), and 11,8% (Brazil) of the total. Thus, if these spaces aimed at the encounter between academics and practitioners, accountable actions were quantitatively addressed on a lower scale. Intelligence has many fronts and topics, but the main production of those Journals related especially to strategic/security studies, professionalization, and intelligence methods and organization. This pattern suggests that academics tend to act as stakeholders; working as a complementary expertise group for practitioners (Arcos, 2013).

3.8.b. Releasing secrets and whistleblowers

In our cases, while freedom of speech and the media are guaranteed in the Spanish and Brazilian Constitutions, the access to certain matters, like national security, is denied according to legal grounds (see Judicial control in section 3.6). This makes it difficult for media to access government data and information, especially when it comes to intelligence. In addition, Spain has no legal framework for allowing declassification of intelligence information, which therefore remains a challenge for media and journalists. On the other hand, intelligence services might prefer certain media actors instead of others to establish a relationship. In Spain, the intelligence services coverage is greater in the case of ABC and *El Mundo* when compared to other media. This is probably explained because other actors, such as independent leftwing *El Diario* and *Público* tend to be more skeptical regarding the intelligence information, while the former ones might echo official narratives, legitimating intelligence efficiency and policies. In both cases, those positions oscillate in a spectrum comprised by the capture of the media by an official or governmental actor, and the independence and investigative mission of the media as ideal typologies that pave the road to the interaction between journalists and intelligence practitioners. This encapsulates an array of situations in which the media can even lose the ability to scrutinize and gain access to information, in some cases being obligated to hold back information or to lose interest in scrutinize intelligence.

It is reasonable to protect the information, especially in the case of policy objectives, sources and methods to conduct operations, location of liaisons and personnel, or information that can really hamper the political stability of the country and the foreign relations with other states (as mentioned in the case of the

Brazilian National Intelligence Policy). Yet, those arguments should not serve to classify and maintain every intelligence action under secrecy. For example, in the 80s, not disclosing the names of intelligence operatives during the SECED years may have been acceptable; but to subsequently classify as top secret information that protects officials who were informants during our current era is misleading. Moreover, classifying information to potentially cover corruption, incompetence, abuse, and even criminal activities is something that can be reverted by the media role. In the case of authoritarian past attached to security, as in Spain and Brazil, over-secrecy has a negative effect to legitimize core state functions. What is worst, it can lead to indifference or tolerance to all the policy actions promoted by the Executive despite their effectiveness. Traditionally, Spanish public officials were under no legal obligation to open their books, reports, or statistics to the inspection of citizens aside from the information conveyed to build policies and by the initiative of the own administration. In short terms, the demonstration of transparency was passive rather than active. This logic was regulated by the principles of access to information but the procedures are mediated by third agencies within the government and conducted at a slow pace (Moretón Toquero, 2014). Naturally, intelligence is an exception to information access. Thus, the media has an essential role here to cover an area that escapes from principles that apply to other scopes of the government.

Another challenge for the media is to know how to deal with classified information. In Spain, journalists should report the finding of secrets documents to the government, but the Official Secrets Law does not specify measures in case of disobedience. However, illegal disclosure of documents can be prosecuted by charges of espionage and treason. Article 584 of the Spanish Criminal Code mentions "helping a foreign power, association or international organization, by falsifying, disabling or revealing information classified as reserved or secret, to harm the national security or national integrity, will be punished as treason, with the penalty of imprisonment from six to twelve years." This creates a legal barrier that must be weighted by the informant and the media journalists that receive sensitive information. In addition, professional secrecy to reveal secrets and protect sources can become a double-edged sword. Although it ensures compliance with the fundamental right to transparency, in some cases, it disseminates information that cannot be checked or contrasted. One example of this dilemma happens when

> The data offered is rarely supported by auxiliary documents, so we [the journalists] have no choice but to trust blindly in the accuracy of the information. We should not be surprised, in this way, the abuses, the lack of rigor, and, to some extent, the predisposition towards the defense of all kinds of conspiracy theories (Falque, 2005, p. 31).

Despite the problem of reliability and validity of information, the media can protect its sources in the same way intelligence protect its operatives. The media can use professional codes to protect witnesses even when they are demanded to reveal sources by enforcement authorities. In 2019, Brazilian journalists received leaks revealing that Judge Sergio Moro colluded with attorneys to prosecute politicians including the former president Lula da Silva. The revelations also questioned the legality of the biggest anti-corruption operation in the country: *Lava Jato* ("Car Washing"). The messages were leaked to *The Intercept Brazil*, an investigative newspaper founded by Glenn Greenwald, the same journalist that published the Snowden revelations in the British newspaper *The Guardian* in 2013. In 2019, after the publication of the messages, Greenwald was indicted to reveal the sources of the information, but he alleged professional secrecy and convoked freedom of press rights to protect informants and whistleblowers.

Whistleblowers are individuals who might commit mistakes or work to obtain self-benefit. Yet, they can act by different reasons and sound the alarms when they are facing unlawful acts in the public or private sector. It is common that they become targets of attacks and retaliation. Thus, some countries have passed laws to protect whistleblowers. For example, Directive 2013/36/EU of the European Parliament and the Council provides for whistleblower protection based on further measures such as the Directive 2019/1937 on the protection of persons who report breaches of Union law. The regulation recognizes the importance of those people as a result of recent scandals such as Dieselgate, Luxleaks, the Panama Papers, and Cambridge Analytical. According to the Directive, these cases show that whistleblowers can play an important role in uncovering unlawful activities that damage the public interest and the welfare of citizens. The text indicates that the media can select whistleblowers as a means of disclosure, particularly when authorities collude with the accusation. However, the Directive does not apply in cases of national security. In this case, if the Member States decide to extend the protection provided under the Directive to further areas or acts, which are not within its material scope, "it should be possible for them to adopt specific provisions to protect essential interests of national security in that regard". Hence, parallel mechanisms to protect whistleblowers still need to be developed even in exceptional areas such as intelligence. In previous sections, we already commented on the importance to create internal controls and Ombudsman figures working alongside judicial courts to receive legal complaints from citizens affected by intelligence activities. In that effort, there must be protection and the opportunity to whistleblowers to reveal wrongdoing within security agencies in Spain.

In Brazil, after the operation *VazaJato*, law proposals to protect whistleblowers reacquired attention. Bill no. 3.165/2015 by Deputy Onyx Lorenzoni aimed to establish the Disclosure Incentive Program of public interest information. The bill justifies that "reprisals against whistleblowers should be

characterized as another form of corruption", thus, it supports "the protection of information revealed by leaks" and "the prohibition to disclose the author of the leaks." The Bill was restructured in 2019 and still needs approval by the Congress. Another proposal is Bill 13.608/2018. It mentions, "The Union, States, and Municipalities should reward those who stand, reject, or investigate crimes and wrongdoing in the administration." However, the legislators did not specify the kind of reward to whistleblowers. Even if the proposals pass the law-making process in the legislative Houses, they do not address intelligence and national security scopes. Thus, in those domains, whistleblowers probably will continue to use the media as a safer channel to reveal information.

In light of that, the clashes between the media and intelligence are just one type of interaction between these actors. On the other hand, journalists covering intelligence and security issues depend significantly on information provided by intelligence agencies and other government institutions. Nevertheless, exclusive reliance on official government sources represents an "adulteration" of the media coverage. In essence, "the media become the government's voice rather than its vehicle of communication" (Matei, 2014, p. 86). Moreover, the media may self-censor, refraining from questioning issues and policies brought up by other media players and by the government. For example, while human rights groups alerted about the existence of the CIA Flights in the early 2000s, some groups of the media in Spain called for thorough investigations regarding fundamental rights violations (see section 3.5). Meanwhile, other newspapers echoed the voices of security agencies who tried to deny those flights to mitigate the outrage in the public. Thus, media can spark or restrain the clarification of wrongdoing by the government and intelligence.

A plausible explanation to this oscillation is that major newspapers receive large government subsidies that might encourage self-censorship. Yet, this is not an absolute rule. For example, during the Catalonian referendum in 2017, the Catalan Government sponsored local newspapers and public radio and television networks that were reluctant to root out and reveal wrongdoing within the government (Santamaria Guinot, 2017). The same logic of protective funding and polarization applied in the case of TV channels rooted in Madrid (Esteban Tejedor, 2018). In addition, Spanish major political parties forbid public and private television to access their executive meetings in political campaigns and they had exercised clientelistic policies to regulate broadcasting concessions (Fernández-Quijada & Arboledas, 2013). This affects media coverage in a priori terms, refraining its independence or imposing tacit forms of self-censorship to expose and construct stories. In Brazil, the major newspapers also receive significant funds from the government, but they are especially concentrated in a media conglomerate of editorial and entertainment business that contributes to the self-restraining effect of media (Marinoni, 2015). The oligopoly structure in the press was consolidated in the 1980s and has little changed until today, establishing a

central system of few private national networks (i.e. Globo, Abril, Folha, RBS, Bandeirantes). It has been said that in the circulation of information specific to this industry, Brazilian agencies act less as de facto news agencies and more as content resellers (Moreira, 2015).

Media moguls can act as advocacy collision groups to defend their position and editorial policies to interpret the situation of the country. In Brazil, during the political turmoil and protests in 2013, and during the Presidential impeachment in 2016, there was a tendency to support the reduction of the governmental apparatus and to demonize policy-makers (Davis & Straubhaar, 2020). That support paved the road to the crisis of the polity but also of traditional media forms as sellers of content. For instance, during the last presidential elections, the political campaign was influenced by social media sources, including the use of bots and algorithms (Soares, Recuero, & Zago, 2019). Those methods alone did not hijack democracy. Rather, they helped to increase a scenario of informational uncertainty that was better exploited by small groups of electoral "soldiers" who planted uncertainty, including false content. Besides the pulverization of information, one must also consider the old dilemma of vast business conglomerates, which often include media firms, as those can enable tight government or corporate control of media ownership. This results in a double effect.

On the one hand, it reduces variety in media coverage and opinions, reinforcing corporate interests, and the politicization of the media. On the other hand, the pulverization of information (which paradoxically increases whereas the media industry becomes more concentrated) also reinforces capillarity to reach more audiences, redefining the relationship between producers of content and consumers. In the case of Spain, Pedro Gonzalez has observed that the existence of conglomerate groups redefines the role of the media in the eyes of politicians and big companies. "They know that if a plausible report is fed to the radio station of any media group, then the TV station and the newspapers of the same news corporation will follow, spreading the story rapidly" (in Matei, 2014, p. 95).

In parallel, the pulverization of information and automatic spread of news refrain the check of information, in such a way as to pass on the report as true, even when it is false. Thus, false or fake news can be understood as real in the minds of listeners, viewers, or readers, and it can become impossible to refute it. Thus, some scholars have mentioned that fake news opens a window to new information literacy, as readers and consumers must be able to filter and recognize different sources (Fernández-García, 2017). In that sense, the problem per se is not the decentralization of the sources of information, but the forms to transmit and consume it. This becomes evident in a hyper-connected and accelerated environment, where media may broadcast chains of information among different conglomerates to retell stories that cannot be always checked, causing loss of

reliability and reputation to the eyes of the public. In turn, this encourages the expansion of alternative sources of information beyond the traditional media.

On the other hand, the media cannot be impartial by essence. Communication is always inserted in a specific political and social environment. Yet, despite the inexistence of neutrality, sensationalism is another element that should be avoided. In that sense, journalists might express extreme personal opinions, sometimes highly biased and speculative, rather than reporting the facts. Moreover, "tabloid journalism" tends to focus on sensationalist topics such as gossip and defamatory columns about the personal issues of public figures. In doing so, the media accountability mission and its credibility might be undermined. In the meantime, advances in technology may increase the availability of information by independent media. However, Caparini (2004) affirms that the media depends on intelligence services for sellable material. Thus, if the volume of articles in security or intelligence has increased in the last years (as seen in Figures 11 and 12), this growth is not necessarily translated in better coverage and scrutiny of intelligence.

In short, traditional media is not dead, as it increases its range and production of contents and stories, especially in the hands of commercial conglomerates. However, in functional terms or in order to foster accountability principles, the media presents many dilemmas and limits as discussed above. At the same time, alternative sources of information had also emerged and must be examined as new mechanisms of accountability as well. This is the case, for example, of WikiLeaks.

3.8.c. WikiLeaks

WikiLeaks is an international non-profit organization that releases news, leaks, and classified information supplied by anonymous sources. Until 2016, the organization has released 10 million documents. Julian Assange, an Australian Internet activist, is described as its founder and director. WikiLeaks documents include video logs from 2007 showing civilian casualties provoked by occupation military forces in Iraq leaked by the former intelligence analyst Chelsea Manning. In 2010, WikiLeaks also released the USA Department of State diplomatic "cables". In 2011, WikiLeaks started to publish 779 secret files related to the detention of prisoners in the Guantanamo. According to its website, "WikiLeaks mission is the revelation of truth […] WikiLeaks relies on the power of uncovering facts to empower citizens and to bring corrupt governments and corporations to justice."[73]

[73] *WikiLeaks*. 2011, May 07. 'About, what is WikiLeaks?' Retrieved from: wikileaks.org/About.html in 11/05/2019.

Since 2010, WikiLeaks has also released material mentioning the Spanish and Brazilian intelligence agencies. The Global Intelligence Files of the website retrieves 216 results and press notes that include the word "CNI" until 2019. For example, on July 31, 2011, the database mentioned that the Spanish government tried to stop the financial activities of Islamic groups in Spain. The action was allegedly important to refrain terrorism support from individuals in the Maghreb and the Middle East. In those documents, the CNI reported that those financial funds were causing negative social consequences, such as the emergence of parallel societies and Islamic ghettos. In that year, CNI press reports mentioned that the economic intelligence division was investigating possible attacks from Anglo-Saxon companies. The alleged companies were supposedly speculating in the Spanish stock market, challenging the financial stability of the country. In addition, other documents from November 28 announced that the CNI was working against the infiltration of criminal cartels from Colombia. The same database contains 42 files of the Italian company "Hacking Team" related to the CNI. Most of those documents are emails exchanged between the company and security partners, such as the National Police and the CNI. The documents reveal technical negotiations and contracts to sell surveillance technologies in Spain. The CNI always claimed the legality of those contracts.

In the case of Brazil, the same method could be applied to the word "ABIN". Until 2019, 241 results and press notes are retrieved in the section "Global Intelligence Files" and 116 results are obtained for the section "Hacking Team". In the first section, diplomatic cables from 2005 mentioned that the ABIN monitored indigenous communities as well as Al Qaeda operations in Brazil with information obtained from USA intelligence partners. In 2019, the section mentions the internal reconfiguration of the Agency in the face of the Supreme Court wiretaps scandal, in which justice authorities were spied by the Executive in the context of the investigation of clientelism, prevarication, and collusion among meat companies and the President Michel Temer. Another document mentions the payment of the ABIN to subscribe to the American strategy magazine Stratfor. In the second section, the files mention that the Italian security company "Hacking Team" sold espionage software to police authorities to be used during the Olympics Games in 2016. In one of these files, the Federal Police would have started using the software one month before the sports event.

In the WikiLeaks database[74], other sections refer to Spanish and Brazilian foreign policies that are not directly related to intelligence. Yet, the above findings are examples of the coverage of WikiLeaks across the world, including our cases. For some intelligence practitioners, WikiLeaks compromised the security of operations and foreign relations with allied countries. Meanwhile, Assange was considered a hero for activists of Internet rights and access to information. Beyond

[74] Retrieved from: https://search.wikileaks.org, consulted in 11/06/2019.

the dichotomy between demons and heroes, the organization has been extensively analyzed by scholars such as Roberts (2012). For him, WikiLeaks failed to promote transparency as a sufficient element to achieve the accountability of governments. That is, transparency does not necessarily enhance accountability; it does not entail profound participation of the citizenship after leaks and revelations. For Davis & Meckel (2013), the organization fails to promote action in the people, especially because this movement is not a social movement and because the internet is not a global common platform.

> Assuming individual decision making as a prerequisite for collective action, decision theory provides little support for the claim that WikiLeaks provides for political accountability. Even if a number of individuals came to the conclusion that government behavior required some negative sanction, WikiLeaks does not help them to solve basic coordination problems. […] The structural problem is not only the information asymmetry between the government and publics (or agents and their principals) but also that principals 1) are unaware of the preferences of other principals; 2) may have a variety of incompatible preferences; and 3) have no automatic incentive to act on behalf of the collective. Massive leaks of confidential, intra-governmental communication to the public do not alleviate these impediments to collective action (Davis & Meckel, 2013, pp. 474-475).

Even if individuals are aware of their preferences regarding policy issues covered in the leaked documents, the volume of data might pose a disincentive to individuals otherwise interested in evaluating government performance. In that sense, WikiLeaks not only fails to provide for accountability but also is insufficient even for transparency. Institutionalized and professional procedures are required to decode data into information that could be useful to support individual and collective action. Other problems in the accountability capacity of the website stem from the personification of the organization around Julian Assange (a direct attack and his imprisonment in 2019 lead to a decrease in the communicative range and political image of WikiLeaks). In addition, the organization did not predict that governments and administrations, despite the momentary embarrassment, recovered confidence releasing counter-narratives or readapting themselves to new procedures of transparency, such as releasing thousands of technical files in transparency websites. The bulky information makes it difficult for any assessment on the side of a regular citizen. Thus, the emulation of WikiLeaks, even by institutional websites comes to demonstrate that "total transparency" is not enough to spark accountability and that leaking for the sake of leaking is ineffective. "Leaking itself neither provides for the contextual information necessary for an informed public nor facilitates new forms of political participation" (Davis & Meckel, 2013, p. 479).

However, WikiLeaks will be part of history because it was one of the first global attempts to counterbalance the opaqueness of institutions including some intelligence services. The strength of WikiLeaks was its initial promise, not the ending actions or the inevitable decline of the organization. In other words, organizations from the civil society like WikiLeaks act like mechanisms that could spark accountability in the initial moments of their revelations. Their major impact tends to occur after leaks as they shed light upon wrongdoing and scandals. Yet, as many civil organizations committed to change politics, their ending goals (and the meaning that the revelations follow) are opened to continuous reconfigurations by other media players and by the reactions of the organizations whose content was leaked. In that sense, this societal strategy has limited value but an essential role that can complement and oxygenate permanent accountability mechanisms. In that effort, the connection between informal or sporadic forms of accountability with institutional or permanent ones is a challenging exercise.

Finally, beyond the role of the media and whistleblowers, another front has been opened by civil society many decades ago. It refers to literature, and fictional stories produced by journalists and writers. Even fictional production is important to interpret the role of intelligence and its relationship with a broader audience, beyond practitioners and scholars.

3.8.d. Fiction and writers

In Literature Theory, Wolfgang Iser affirms that fiction, reality, and imaginary are related through what he calls "the act of pretending". According to him, the author of a fictional artifact embraces reality, firstly, by choosing themes, aesthetics, events, feelings, among other aspects. Then, she/he builds a narrative combining the elements captured from reality, transgressing the limits from it. Finally, the author presents another world in the narrative, which is a "represented world" (Iser, 2002, p. 956). He emphasizes, in this operation, the importance of the imaginary as an "experience of happening", which permeates the perception of what we understand to be the real world, shaping and reaching the sensibilities and imagination of readers or viewers. Hence, the actual vs. imagined/constructed tension shapes our visions of reality to some extent.

In that sense, many readers can have their interpretation of politics and social practices altered even by the assimilation of fiction. In the case of intelligence, they might be attracted by issues such as honor, discipline, darkness, conspiracy theories, and so on. For this reason, journalists and publishers had been efficient to put this type of product in the market, even in the form of documentaries. The literature related to intelligence services is vast especially if we consider the operations and activities conducted throughout history. In Spain, for example, *La Casa del Cesid: agentes, operaciones secretas y actividades de los espías* (1993) by Fernando Rueda is the foremost publication about espionage

episodes of the CESID before it became an object for the media and the Parliamentary Commissions. More recently, he wrote several bestsellers such as, "Las Alcantarillas del Poder" in 2011 (The Sewers of Power) "El Regreso del Lobo" in 2015 (The Return of the Wolfe), and "El Dosier del Rey" in 2017 (The King Dossier), literal translations. Given the editorial success of such kind of publications, other books appeared following the same plot. Mikel Lejarza and Elena Pradas are other authors who promoted the espionage-intelligence marriage in Spain (Falque, 2005), as in the case of "Yo Confieso: 45 años de Espía" (I Confess: 45 Years as a Spy, literal translation). Most of those books tell plots in which agents of the CESID are inserted in a narrative of deceiving, wiretapping, and covert actions. Other books are more historical and a sort of synthesis of the espionage in Spain, such as *Servicios Secretos* (Secret services, literal translation) released by journalists Joaquín Bardavío, Pilar Cernuda, and Fernando Jáuregui in 2000. In 2019, Cernuda interviewed and released a book based on the story of female spies in Spain entitled "No Sabes Nada Sobre Mí" (You Don't Know Nothing About Me, literal translation). In Brazil, some examples are *Ministério do silencio: a história do serviço secreto brasileiro de Washington Luís a Lula* (Ministry of silence: the history of the Brazilian secret service from Washington Luís to Lula, literal translation) published by Lucas Figueiredo in 2005. This author aimed to realistically summarize the evolution of the Brazilian intelligence in the last century. More examples are *A contra-espionagem brasileira na Guerra Fria* (Brazilian counterintelligence in the Cold War, lit. trans.) written by Jorge Bessa in 2005, and *Ex-agente abre a caixa-preta da ABIN* (Former agent opens ABIN's black box, lit. trans.) published in 2015 by journalists Andre Soares and Claudio Tognolli and by the former director of the Federal Police, Romeu Tuma. Even Brazilian soap-operas (telenovelas) such as *Poder Paralelo* (Parallel Power, lit. trans.), written by Lauro César Muniz and directed by Ignácio Coqueiro in 2010, portray a corruption and investigative plot inspired by the actions of *Satiagraha* operation in a more fictional fashion.

In those and other examples, fiction comes to depict a popular image that involves intelligence and secrecy. However, the mystery and shadows surrounding these organizations are not dissipated insofar as many actors (even the media coverage) tend to use these allegories as "common ideas" to refer to intelligence services. In that sense, it does not mean that fictional stories are inferior or should be avoided by the regular reader, or that fictional stories have nothing to tell us about intelligence. Even real intelligence agencies work thanks to the use of real fictions based on security grounds and missions, let alone the potential use of information and "disinformation". Every sociopolitical order endures thanks to meta-fictions to rule a country or to coalesce a nation.

Rather, it means that traditional fronts to scrutinize intelligence, such as the role of media, should consider but not mistake the mental images that are used to construct literature and novels. In the case of realist novels or documentaries,

journalist resembles the work of historians and the analysis of historiography. In this field, the production of testimonies, memory, facts, and assessment of the past is hampered by limitations established by secrecy from the official power. Thus, the most important thing for the proper methodological development of the Spanish historiography referred to the intelligence services is that new mechanisms of declassification need to be established, to overcome the bureaucratic inertias to access the documents from the past (see rules of declassification of information in section 3.6). The overproduction of literature tends to repeat the archetype of "mystery, secrecy, hidden power, heroes, demons, and conspiracy elements" to intelligence. Thus, the journalist, as the historian, must confront with great caution the information coming from sources of first hand.

In the case of historians, Hayden White expresses that, when historians look into the past, narratives would be produced by the search for truth, but without losing the ethical and political dimension of the historian craft. He highlights the relationship between writing about the past and the demands of the present in which the historian lives. This would be a way of valuing the critical potential of the historian and his/her production, connecting the past with the present society in a broad sense, not only with a specialized audience. Literary writing, for White, is close to historical writing, although there are clear differences - in terms of form and objectives - between them (White, 2014). Different from history, literature - and other fictional productions- can rescue the historical past with objectives that not necessarily embrace ethical and moral reflections to readers or viewers.

Historians also can use fictional and literary sources but they need to interpret those sources with accuracy since one of the issues related to personal testimonies of past events is the subjective and ever-changing characteristic of memory. This is not a position in favor of a positivist history where facts are the only important element to produce stories. Rather, as the future is always unknown and remains in the "becoming", memories are always changing. This is because the past is always opened to reinterpretation and to receive new futures. Besides, what testimonies and stories omit or silence could be more transcendental than the speeches and words. The ideal receipt to deliver a story might not exist. Yet, for novelists and historians that construct a reliable story, it would be wise to compare the written/oral testimonies with declassified secret documentation. Unfortunately, the triangulation of information between unofficial memories and official sources is still very scarce in the Spanish and Brazilian historiography, especially by the rules of declassification and the legacy of authoritarian periods (see different kinds of historical memory in Section3.2).

Epilogue

Intelligence services need the media to oversee and legitimize their security activities. Hence, the press has a great role and makes a significant contribution to the control and oversight of intelligence in these points: to inform the general public; to connect government with the citizens; to boost government legitimacy; to exercise informal external oversight of the government; and to provide a "learning" environment for elected officials and the public (Matei, 2014).

In this section, we have seen the coverage of the major newspapers in Spain and Brazil regarding intelligence activity. In that coverage, the media sometimed acted as a mechanism of transmission of classified information that internal practitioners put at the disposal of journalists. In that sense, the media contributed to dodge rules of declassification. For example, in Brazil, in 2005, media leaked information about the Satiagraha Operation, a federal investigation conducted by the Federal Police and the ABIN that involved illegal wiretapping of politicians, ministers, bankers, public servants, lawyers, and judges. In Spain, in 1995, Juan Alberto Perote, the head of the Operations Group in the "Centro Superior de Informacion de la Defensa" (CESID) leaked 1200 documents from the intelligence service. The CESID papers revealed illegal wiretapping by intelligence services to politicians, journalists, and other public figures. Both episodes redefined the forms of control of intelligence services and the political life of those countries.

In the meantime, the media and intelligence have a relation of "love and hate". They can mistrust each other (and they should), but they also depend on the other to improve their legitimacy or to release a story. Those positions oscillate in a spectrum comprised of the capture of the media by a governmental actor, and the independence and investigative mission of the media. This spectrum encapsulates an array of situations in which the media can even lose the ability to scrutinize and gain access to information, being in some cases obligated to hold back information or to lose interest to scrutinize intelligence.

Moreover, journalists covering intelligence and security issues, which are otherwise hard to access due to secrecy, depend significantly on information provided by intelligence agencies and other government institutions. Nevertheless, exclusive reliance on official government sources has negative consequences. In essence, the media can become the government's echo rather than a vehicle of communication. The latter trend increases insofar as the concentration of the media increases in a handful of large holding groups. In Spain and Brazil, this kind of concentration entails self-imposed censorship that could focus on sellable stories and descriptive coverage, rather than on substantial production of news to scrutinize the intelligence activity.

On the other hand, both in Spain and Brazil, other groups of civil society such as scholars have discussed the role of intelligence. However, considering the academic role, the percentage of scholar and professional articles addressing accountability regards only to 12,4% (Spain) and 11,8% (Brazil) in the main journals. Thus, accountable actions were covered by this group but only on a lower scale. For this reason, it would be valuable if intelligence services open their institutions for deeper reforms. They might discuss with society the directives and overall goals of intelligence every year, showing to citizens that the agencies work according to the legal framework imposed by the elected policy-makers but also by considering the interest of the public. In that sense, the real inclusion of a wide spectrum of groups, opinions, and perspectives (from practitioners, experts, academics, to non-experts) in new commissions to assess general aspects of intelligence and national security policies may result in a real improvement of their legitimacy.

Regarding the role of citizens, even "pop culture" and fictional stories have something to say. The mystery and shadows surrounding these organizations might be dissipated as "common ideas" to refer to intelligence services. In that sense, it does not mean that fictional stories are inferior or should be avoided by the regular reader, or that fictional stories have nothing to tell us about intelligence. Even real intelligence agencies work thanks to the construction of "serious" fictions. Rather, it means that traditional fronts to scrutinize intelligence, as the role of media, should consider but not mistake the "common ideas" that are taken to build news and stories. In that effort, journalist resembles the work of historians and historiography, a field in which the production of testimonies, memory, and the assessment of the past is essential. Yet, the work with the past and the elaboration of stories is hampered by limited mechanisms of declassification of official information, especially in Spain.

So far, we have expressed the main aspects of accountability in the role of media and civil society. Those aspects are represented below in Table 14. At this point, what are the overall mechanisms and principles enhanced by this kind of accountability?

In Spain and Brazil, the CNI, the ABIN, and the government in a broad sense are accountable to media and civil society. Those actors can address the intelligence services to describe general policies, to clarify political scandals, to notify institutional changes – such as the replacement of Directors and the modification of budgets and Ministry adscriptions. However, media and civil society do not formulate substantial coverage regarding the formulation and evaluation of policies, the functioning and specific goals of intelligence (most of the time as a consequence of secrecy), and the disclosing of information (especially in the case of Spain).

Intelligence services and the government as a whole are accountable by direct and indirect means. In the first point, the services can reveal information or give official communication to media players. They also can release documents and reports on official websites, and even establish Public Relations departments and parallel media channels. Moreover, when the media address intelligence, it could become, on the one hand, as echo-chambers transmitting intelligence policies rather than a vehicle of communication. On the other hand, the media can develop independent and investigative stories that can scrutinize the government more deeply. Yet, the latter dimension can be restrained by the dependence on official information to release stories. Besides, the investigative role can be reduced because of the concentration of vehicles, such as television and newspapers, in the hands of a few corporate groups with their specific agendas.

Nevertheless, investigative and ethical journalism is not dead and can be reinforced by indirect mechanisms of accountability. One of these mechanisms is the role of whistleblowers, exemplified in the major political scandals of intelligence in both countries. Other mechanisms are institutional forms to release leaks and revelations at the national or international level, as in the case of WikiLeaks. In addition, academic journals might constitute spaces of exchange of ideas and dialogue between practitioners and scholars from different areas. Finally, even popular culture and fictional narratives contribute to the formation of an archetype of intelligence. By doing so, they put these services on the radar of the communicative action of general citizens.

Table 14: Accountability in the role of the media and civil society

Accountability dimensions	Cases	
	Spain	Brazil
Who is accountable?	National Intelligence Agency (CNI) and the government in a broad sense	Brazilian Intelligence Agency (ABIN) and the government in a broad sense
To whom are they accountable?	To the media and civil society	To the media and civil society
About what are the services accountable?	More addressed: *- general policies* *- political scandals* *- institutional changes* Not addressed: *- formulation and evaluation of policies* *- functioning and goals of intelligence* *- disclosing of information*	More addressed: *- general policies* *- political scandals* *- institutional changes* Not addressed: *- formulation and evaluation of policies* *- functioning and goals of intelligence*
How are they accountable?	Direct means *- Official communications* *- Media as echo-chambers* *- Investigative and independent media* Indirect means *- Whistleblowers* *- Leaks and revelations* *- Scholars and journals* *- "Pop culture"*	Direct means *- Official communications* *- Media as echo-chambers* *- Investigative and independent media* Indirect means *- Whistleblowers* *- Leaks and revelations* *- Scholars and journals* *- "Pop culture"*

Assessing accountability according to its internal principles	Did the accountability action result or promote at least one of the following principles? -Answerability -Transparency ~~-Responsibility~~ ~~-Enforcement (punishment)~~	Did the accountability action result or promote at least one of the following principles? -Answerability -Transparency ~~-Responsibility~~ ~~-Enforcement (punishment)~~

Source: author

The performance of public accountability as a connector between authority and legitimacy is a question of interest in the role of the media and civil society. When authority is called to give an account, if that action does not entail more legitimacy, then accountability fails to reach its objective. In that logic, when an authority from intelligence is called to be accountable in this domain, it is possible to speak of accountability especially by answerability and transparency.

In the first logic, the media could spark accountability by answerability. Yet, it lacks sufficient strength to demand responsibility (to inculcate duties and change direct policies) and enforcement (capacity to sanction or judge official authorities). Despite being an example of vertical accountability (a relation between unequal powers or asymmetric actors), we have shown how the Parliamentary Commission for Reserved Funds in Spain and the Parliamentary Commission for the Control of Intelligence Activities in Brazil have used information from newspapers and the media to demand justifications and explanations from the Executive. This is because the informal oversight carried out by the media usually occurs through the lens of scandals, such as the exposure of human rights abuses, misappropriation of funds, or other violations that may force formal accountability mechanisms to do their job more effectively. In that sense, the role of media and civil society can start judicial investigations, and even change legislation. Despite the limitation of informal accountability mechanisms, they can activate justifications, explanations, corrections, and even modifications in intelligence. This is the case of scandals covered by the media before the institutional reform to update the intelligence agencies in Spain (2002) and Brazil (1999). The media coverage during events such as terrorist attacks (as attested by figures 11 and 12) also served to replenish the role of intelligence towards the general society. Thus, media is not a precondition to answerability but it can boost this accountability principle in different situations.

In the second logic, investigative journalism, and indirect forms and accountability (whistleblowers, leaks, and revelations) can work for the sake of transparency. We discussed the case of WikiLeaks to enhance transparency as well as its limitations. Compared to other mechanisms of accountability, the media and civil society, as actors with less power before the state, use their asymmetric position to shed light upon the "dark" areas of government to foster transparency and reveal "what is happening/what has happened". Transparency works as a complementary and valuable tool of accountability that is scarcely used. This principle has a tremendous impact on a sensitive arena of secrets. Nevertheless, as

discussed in the theoretical framework, the illusion of total transparency is misleading to assess accountability, and transparency should not be mistaken with accountability as a whole. In the case of WikiLeaks, for example, it is evident that it failed to promote transparency as a sufficient element to achieve the accountability of governments. That is, transparency is not necessarily a condition to accountability; it does not entail automatically the mobilization and the participation of the citizenship after leaks and revelations.

Nevertheless, transparency mechanisms from the civil society are stronger accountability mechanisms in certain situations, like in the initial moments of revelations. For example, the major impact of leaks tends to occur after their revelations as they shed light upon "wrongdoing". Their strength, hence, consists of the initial promises and the capacity to inculcate ulterior action in other citizens. In citizen strategies dedicated to change politics, the ending goals and the directions are always opened to continuous reconfiguration and adaptation by other social players. In that sense, the media and societal strategies have a limited range in terms of scope and temporality. Moreover, their role depend on institutional actors to redefine other institutions, such as intelligence agencies. However, the media and civil society actors have an essential role that can complement and oxygenate permanent accountability mechanisms, as the ones we exposed in the previous sections. In that logic, it is important to remind that societal actors are directly involved in the construction of legitimacy. The people from civil society are the direct source of legitimate power. And this kind of power is something that any public authority and institution should retain.

Chapter 4. Surveillance and intelligence: connecting the points

In the previous chapter, we have seen that different mechanisms of accountability have emerged to oversee intelligence. From the creation of information services for the repression of dissidence in the 1960s to the current international cooperation for the analysis of globalized phenomena, intelligence has changed in multiple connotations and sectors (see the increasing roles of intelligence in Section 3.4). Yet, when conducted in strategic agencies for the security of the state (as in the case of the CNI and ABIN), intelligence also refers to watch and process information, including data from populations. In other words, the strategic intelligence for the security of the state has many tasks, but it also can be considered as a form of surveillance. In that sense, intelligence theories and practices still need to be connected to surveillance.

We have shown that intelligence was formulated as a process, as an organization, and as a form of knowledge to reduce the complexity of information for high decision-makers. Yet, scarce mention is given to intelligence as a privileged form of state surveillance. In addition, surveillance can help to revisit the role of intelligence and the role of citizens that are submitted to this activity. It does not mean that every form of intelligence aims to surveille individuals. Yet, since this activity has this potential, we still need to think in new forms to tame the power of surveillance-intelligence. That is, when we think outside the traditional intelligence box, it is possible to enrich the analysis of this field, showing new points of connection between close, yet distant fields.

In order to connect intelligence and surveillance, it is important to recall our concept or understanding of surveillance as presented in Chapter 1. In that sense, surveillance is the continuous socio-technical interaction or activity addressed to collect, process, and refine information from/to certain objects with concrete or diffuse purposes. This phenomenon ranges from the mediation of power through the gaze and the self-discipline of subjects (panoptic metaphor), to the gaze as a site of nodal power (rhizomatic assemblage metaphor) that mediates the transition between exceptionality and normality circumscribed to the objects of surveillance (the watched). As surveillance is connected to the panoptic and the rhizomatic assemblage, it also consists of the regulation of life cycles, development, and growth of individuals (biopolitics), and of the management of populations with the aim to constitute and sustain the dispositives that coalesce and operate the techniques to select, sort, classify, categorize and govern the heterogeneous “mass” of people (governmentality). Thus, surveillance does not equalize a relationship of power between surveyors and surveilled. It also entails a relation of power that

produces different fronts of reaction and resistance to the mechanisms of governmentality.

Considering that definition, we can simplify or establish three core ideas: there are modes or metaphors to operate surveillance, there is a specific management of individuals in a population, and there is resistance derived from power relations. In turn, those ideas can be reformulated in these points in order to connect surveillance and intelligence:

1) Can surveillance metaphors (like the panoptic and rhizomatic assemblage) work in the realm of intelligence? (Section 4.1)

2) What is the relationship between intelligence and the management of subjects in a population? (Section 4.2)

3) What is the relationship between intelligence and legitimate resistance? (Section 4.3)

The three points allow to connect both fields. At the same time, they are explained because they allow to establish a common ground to reach our study objectives. By answering those points, it is possible to assess the management of individuals' autonomy as well as the power asymmetries between watchers of the state and the watched groups in the population. Naturally, the watched targets in intelligence are many and include other states, public and private organizations, and even potential threats to the state. However, amidst those targets, legitimate dissidence and resistance appear as unexplored issues around intelligence. If resistance can be exercised by means that are not violent, yet by acute intensity and force against the sociopolitical establishment in order to reach greater levels of people's legitimacy (by more responsibility, transparency, answerability, and enforcement), this trend deserves attention from state watchers but also from scholars.

To answer the three points, we do not intend to formulate a measurable scale or a quantifiable impact from the watchers upon the watched. This task would be impossible due to secrecy in this realm. Rather, the points try to update the surveillance theories in Chapter 1 and 2 with complementary analysis and accountability findings expressed in the last Chapter 3. Besides, the connections might be reworked by scholars researching more cases and can be used by prospective studies that address both fields. Let us answer the first point.

4.1. Surveillance metaphors and intelligence

In a first approach, intelligence can be interpreted as a synecdoche of surveillance, a part of the "whole", a field within the broader surveillant assemblage. We are not proposing a hierarchy between those fields and the

submission of intelligence studies to surveillance. It means that both are connected and the former can be deemed as a specific form of surveillance to watch and obtain knowledge in favor of non-common watchers (decision-makers attached to strategic and state organizations that work under secrecy). Producing intelligence does not mean necessarily to surveille someone, but certainly, it entails a form of watching, a series of techniques and operations that are preserved from other organizations.

State intelligence services, the focus of this study, could be labeled as the epitome of official sovereign power in a certain sociopolitical order. This kind of agency was created to help the police and military in scenarios of conflict and internal division such as Spain and Brazil (see the origin of intelligence and authoritarian legacies in section 3.2). The historical and archivist field mentioned in this study confirm that genealogy. In turn, the evolution of the mechanisms of accountability shown in the last Chapter, confirm that intelligence can be associated with surveillance theories and metaphors.

In the panoptic metaphor, the change of a centralized official gaze (to monitor suspects or threats to states) to a more decentralized network to collect information is easily associated with intelligence agencies. From a vertical and top-down institutional infrastructure to the new network of intelligence cooperation with foreign partners, and from the evolution of the intelligence cycle to the flexible-target approach of operational task forces, these changes evidence that the panoptic surveillance has been concentrated in the centralized gaze of official watchers. The organizational and institutional evolution of these services, from reactive and colossal bureaucracies of information to the new interdependence of informational networks, confirm the modulation of the panoptic itself during the last decades in our cases. The decentralization of power, from top-down structures of defense (during the political transition in Spain and Brazil) to new intelligence communities (in the sense that intelligence depends on other administrations and countries to share information), should not be interpreted as a leap to a post-panoptic paradigm.

As mentioned in the theoretical framework, the panoptic metaphor is based on a form of power mediated by the gaze, and, in this case, intelligence can be understood as a form of governance that mediates the gaze of policymakers for the preservation of the sociopolitical order. Moreover, the panoptic entail disciplinary effects over a group of people, regulating normality from abnormality in a flexible fashion. This could be seen especially in the case of criminal intelligence and police intelligence that work to support judicial and enforcement authorities. Yet, even strategic intelligence for the security of the state (the focus of this study) and military intelligence with defense purposes are intertwined in order to identify suspects that can affect or subvert the establishment. Nowadays, this case arises in the example of anti-terrorism, organized crime, international sabotage, internal

insurrection, financial instability, cyber-attacks in infrastructures, the proliferation of weapons of mass destruction, pandemic virus, climatological changes, and so on. All those phenomena entail a "war" against an enemy "who is nowhere and everywhere" at the same time. In that effort, the preemptive logic of intelligence connects it with surveillance, as both deploy rational techniques to identify, sort, and classify certain individuals and groups. These target groups, in turn, serve to regulate a whole population in a territory. Thus, among the plethora of missions and goals, intelligence represents an official form of authority is deployed in each country.

Furthermore, the metaphor of the rhizomatic surveillant can be applied to intelligence as well. In that sense, this activity is also constituted by several fronts or rhizomes, such as administrative levels, institutional configurations, legal mandates, and informal practices. Indeed, when we analyze the institutional design and legislation of strategic intelligence around the world (Bigo, 2015; Gill & Phythian, 2018), including Spain and Brazil (see sections 3 and 4); the legal rules allow connections and promote cooperation with other rhizomes and security agencies. This flexibility is essential to the adaptability of those organizations in a time of rapid changes, increasing interdependence, and uncertain risks. Moreover, since the transition of authoritarian regimes, the performance, and efficiency of these institutions demand to obtain more technology and data sources (i.e. by the creation of the National Cryptologic Center in Spain and the attempt to institutionalize the SISBIN in Brazil). Moreover, intelligence communities have learned that the ontology (exact nature) of threats has changed. The intelligence cycle, as a sequential and rational model, has been influenced by constructivism and the rise of critical theories (Bean, 2018). That means that not only intelligence services are able to read the world, but also to interpret and construct some aspects of reality, from threats to security answers. In simply terms, threats are both factual and constructed, risks are unforeseen but also produced as side effects of human action or as deliberate social impacts (Yauri-Miranda, 2016).

At the same time, after the Snowden revelations, we know that the most developed intelligence agencies in the world were linked to mass surveillance techniques. In this front, the tracking and monitoring of ubiquitous data are as important as intelligence products. We cannot prove that mass surveillance is conducted or shared with the CNI or the ABIN, but the analysis from the last Chapter found evidence that both countries were affected by this practice, from normal citizens to politicians and authorities. The exponential growth of mass surveillance resembles the abstraction of physical bodies into digital flows that are detached, recombined, and processed into new virtual forms of remote control, enhancing multiple opportunities to surveille entire populations.

Thus, the "panoptic" and the "rhizomatic surveillant assemblage" are more than metaphors or figures of speech to analyze intelligence. They represent the

molds and the circuits of information, as well as the expansion and the capillarity of different intelligence networks. These characteristics rise challenges to oversee and control this realm in terms of accountability. Intelligence services such as the CNI and the ABIN are not Big Brother machines that surveille everything and control everybody. Yet, they are central nodes in the rhizomatic constellation of strategic organizations that regulate key flows of information in each country. In that sense, if intelligence is part of the surveillance assemblage, how intelligence is operationalized for the management of subjects and populations?

4.2. Intelligence and the management of subjects

Considering that intelligence agencies are part of the surveillant assemblage, they can be deemed as dispositives to administrate subjects and to regulate the distribution of power in a sociopolitical order. In this perspective, intelligence still preserves its historical feature as an implicit surveillance tactic to modulate (not to concentrate in one single actor) social control. This is because strategic intelligence is linked to mechanisms of normalization and power that are not distributed from a center, nor is it the result of a contract or a formal institution. That is, intelligence is a technique of power that cannot be perceived exclusively by legal or institutional dimensions.

For example, instead of appropriating or subjecting individuals to punishment as in traditional control, intelligence is more similar to a governmentality technique to modulate the performance of individuals and bodies. This implicit technique addresses a series of habits, as in the case of categories of suspicion, and observes targets that could affect matters of geopolitical interest for the security of the state. In that sense, the ideal hierarchical vigilance, whose archetype is the classic intelligence era during the Cold War from which "nothing" can escape has been changed. The current intelligence has implicit mechanisms of coercion that go beyond hierarchical and vertical forms. Like surveillance, it can be shifted to oversee the "productivity" (life, growing, and death) of bodies, preserving the safety of the whole population by targeting samples of the population that represent undesired behavior or threats.

Discipline implemented by harder means (to profile dissidents or individuals who subvert the order, including terrorists) is not necessarily an instrument of enforcement or repression, but an apparatus for checking attitudes and oversee performances in the rest of society. However, as the discussion on surveillance suggests (see Chapter 1), this oversight is not a governmentality technique of homogenization. Rather, it identifies and measures levels to operationalize differences through continuous adjustments, as in the idea of tracking individuals to shape their individualities by continuous adaptations of control (Deleuze, 1995).

Thus, control today is not about homogenizing and correction. It is about flexible oversight of individuals and capillarity to reach differences and habits in many fields (labor, education, personal life, security, and other domains) that can be covered by intelligence in case of suspicion and potential threats.

In that sense, the development of intelligence has reshaped the notion of individuals as targets for surveillance. That is, intelligence, as other forms of implicit control, has also enabled dataveillance (data + surveillance) to focus on humans as species and as individuals, from the big picture of populations to the tiny routines of almost every person (Van Dijck, 2014). To focus on humans and their performance (i.e. habits and productivity), broader databases and information networks are essential to the official administrations. For example, the interconnection with foreign databases in the case of Spain and the institutionalization of the SISBIN in Brazil resemble highly specialized institutions to assess and categorize information.

The activity of intelligence also relates with biopolitics, the exercise of power over personal life to address the population as a whole. In that sense, this field represents the epitome of a set of institutions created to the intervention and administration of the social reality. By watching multiple threats and phenomena, intelligence regulates the promotion of favorable phenomena and the minimization of unfavorable risks to the administration of individualities. Every agency adopts preemptive analysis and balance different scenarios to preserve the integrity of entire populations. In that sense, intelligence is adapted from institutions that promote disciplinary effects to biopolitics to protect the overall people in a country.

Instead of deploying punishment, as during the 60s and 70s in our cases, strategic intelligence has shifted from a disciplinary logic. Today, the disciplinary characteristic of intelligence is secondary. This technique is redundant because individuals might offer themselves as “subjects” (to the state) or as “products” (to the market) to feed the surveillant assemblage. The archetype of security agencies of the state as “saviors” of populations is only valid in exceptional circumstances. In normal circumstances, individuals should “take care” of themselves in the first place. They should oversee their performance and actions. Indeed, the internalization of disciplinary effects, for good and evil, is one component of the panoptic that still survives in the administration of populations. In short, strategic intelligence is still a form of power that acts as a dispositive of control and as a component to modulate biopolitics through secrecy. Nonetheless, at the extremes of these modulations of power, possibilities of resistance are always possible, improbable, and necessary.

4.3. Intelligence accountability and legitimate resistance

If oversight and accountability mechanisms have emerged to restrain intelligence, especially since the end of the Cold War, an important connection still must be pointed between intelligence and surveillance in terms of resistance. But first, we need to consider the virtues and limits of the accountability mechanisms analyzed so far.

As attested by the assessment of the accountability mechanisms in the two cases (internal control, legislative control, judicial control, third dimension control, and media role and society), each of those mechanisms has strengths and weaknesses that can be represented in the table below.

Table 15: Accountability principles mobilized in the realm of intelligence

		Accountability principles			
		Responsibility	Transparency	Answe-rability	Enforce-ment
Accountability mechanisms	Internal control	X			
	Legislative control			X	
	Judicial control (in Spain)			X	X
	International oversight (third dimension)			X	
	Media role and society		X	X (indirectly)	X (indirectly)

Source: the author (based on Chapter 3)

As seen above, almost all the accountability mechanisms promoted at least one principle: answerability. That is, legislative and judicial bodies, as well as the role of international actors, the media and civil society enhanced some capacity to demand "answers" and formulate corrections to intelligence actors by soft means. Answerability relates to trust and checks and balances (equilibrium of power) in contemporary societies. In the case of media and society, answerability was promoted especially by indirect forms, by the combination of other institutional mechanisms (such as Parliaments and Courts). In addition, the media and civil society were essential to promote some degree of transparency to the public from intelligence services. Without the indirect role of the media, leaks, and active involvement of citizenship, many areas of intelligence would have remained out of supervision. The transparency principle relates to some degree of visibility, exposition, and openness.

In the case of the judicial control, accountability depended on the predisposition of courts to evaluate "answers", and to impose corrections by the enforcement principle (constraining the interference of rights and enhancing sanctions by "hard" means). Yet, this mechanism was scarce due to the initial clashes between the executive and the courts. Besides, there is a lack of evaluation of judicial warrants of the Spanish intelligence (In Brazil, judicial control is virtually inexistent). In Spain, secret intelligence materials can be used in courts to incriminate people. These intelligence materials are considered expert evidence to be evaluated by judges and courts only in specific cases involving terrorism and organized crime. Intelligence is not equal to secrecy, but secret information can be originated by intelligence reports. To be used by regular courts, intelligence must be declassified. However, only the Council of Ministers is allowed to declassify secret and confidential materials. Also, there is no definition of national security in the Constitution and whistleblowers in the Spanish Criminal Code. Besides, no specific provision on the use of digital surveillance is included in the legislation in Spain, although it does exist in judicial practice (Bigo, Carrera, Hernanz, & Scherrer, 2015). Thus, the promises of "answer" and corrections by "enforcement", eventually, depends on the predisposition of the executive (and intelligence) to assume its responsibilities. After the role of courts, media and other external actors, the executive needs to enlarge its legitimacy by assuming requests, internalizing changes, and eventually modifying its policies. That is, the executive itself has the last word when it comes to promote and assume responsibility.

Yet, by the analysis conducted in the last chapter, we can mention that the accountability mechanisms have focused on institutional lines and judicial aspects of intelligence control. In the last years, new fronts, such as the role of the media and civil society, have acquired importance to oversee and scrutinize intelligence. However, those fronts remain underdeveloped in terms of scale and scope. For example, little has been done to question intelligence beyond the production of specialized knowledge to high decision-makers in states (or in complex organizations), and as a form to preserve the sociopolitical order.

Thus, to expand the understanding of surveillance and resistance in this realm, it is important to recall the objective of this study:

How accountability can redefine intelligence in terms of

- The management of individuals´ autonomy in a specific population
- The asymmetries of power between those who watch and those who are watched

By autonomy of individuals, we refer to some degree of privacy and auto-representation that individuals adopt in the face of surveyors and within the surveillance assemblage. This level of autonomy is essential to privacy insofar as a lack of this characteristic overrides any understanding of active citizenship and

individuality to construct social relations. Besides, subject autonomy could be related to civil and political rights that are the normative foundations of contemporary sociopolitical orders that refer to themselves as democracies. In that sense, subjects' autonomy and individuals rights must be understood as normative condition to be extended or preserved to the whole population, instead of being restricted to privileged and restricted groups. By asymmetries of power between those who watch and those who are watched, we mean a difference of power that implies a tension between authority and legitimacy (see Figure 5 in Chapter 1). In that sense, the authority of intelligence to "watch" entails a capacity to administrate and regulate populations by addressing target individuals, the "watched". That difference of power is exemplified by the notions of implicit control and biopolitics as explained in the previous section.

To verify if accountability mechanisms can replenish 1) individual autonomy and 2) the asymmetry of power between "watchers" and "watched", one of the biggest obstacles in this study is that it is not possible to assure the specificity and identity of the targets of intelligence. What is worst, considering that intelligence relates to surveillance and the administration of populations by the analysis of individuals' information, the accountability mechanisms expressed in Table 15 have limited potential to promote individual autonomy and to redefine the asymmetry of power between intelligence and the watched people.

This is not saying that intelligence is automatically linked with disgusting or pathological forms of surveillance (un-checked, disproportional, intrusive, inconsequent, and banal collection and use of data) that abolish the autonomy of individuals and increases the power distance between watchers and watched. It means that, if pathological trends of surveillance are potentially conducted by intelligence means, they cannot be effectively restrained by the existent accountability mechanisms. Internal and external controls, from international actors to the role of the media and civil society, oxygenate but do not tackle the structural layer in which intelligence services act. In other words, the difference of power between watchers of the state and the target groups from the general population, and the relationship between authority and legitimacy that hinges around them, presents a considerable gap hard to be fulfilled with current accountability mechanisms.

That gap is explained because the accountability mechanisms depend on each other, on contingency factors (policy opportunities like scandals or polity reforms), and on the predisposition of the accountable actor itself, to be succeeded. The efficiency of accountability, then, depends on a set of factors hard to converge, as the mechanisms (as seen in the last table) cover few principles when analyzed separately. And this is especially true if we consider that the intelligence realm resembles a scenario of huge asymmetric power between the accountant and accountable actors, as the latter (intelligence) concentrate greater amounts of

authority and power to ignore, block, or constrain the actions of external controllers. This does not mean that intelligence is out of control, or that accountability mechanisms have not been improved, but all of them still need to be developed. Besides, since intelligence is a privileged space of the state, and considering that this domain has its inception marked by the legacy of previous authoritarian regimes, few doubts remain in terms of the big difference of power between intelligence services and other actors who demand accountability.

Intelligence has changed during the last decades. However, this realm still represents one of the driest areas to grow efficient accountability mechanisms and achieve more legitimacy in politics. Thus, every form to improve the mechanisms of accountability, as stated in the epilogues from the previous sections, is necessary and essential. This study has also verified that the mechanisms have been improved in their internal logics and many obstacles have been removed since the creation of the first internal and legislative controls in the last century. Also, from a historical perspective, the judicial and societal controls are even more recent and still demand further attention.

To develop societal accountability mechanisms, intelligence remains a closed realm in the surveillant assemblage that constitutes itself as a cornerstone to the sustainment of the sociopolitical order. Hence, new forms of resistance and active citizenship that challenge the sociopolitical order, and their relationship with intelligence, appear as unexplored issues.

In light of that, what is the relationship between intelligence and legitimate resistance against the sociopolitical order?

If citizens can engage against their sociopolitical order (polity and policies that sustain the state) in manners that are no violent and illegitimate, they also can redefine the forms to scrutiny official authorities. Not only they can watch the state to avoid wrongdoing and deviation of authority, but they also can clash against their authorities to foster even more legitimacy of institutions in the sociopolitical order, including intelligence. However, how this kind of resistance could be compatible with an activity that is supposed to protect the sociopolitical order and construct suspicion in groups committed to alter the establishment (even by legitimate means)? Can we speak of radical tactics to reinforce the accountability of intelligence or are both sides diametrically incompatible? If so, are the limits of accountability in this realm fatally dislocated to the above fragile mechanisms of accountability?

Those questions remain unexplored topics for deeper analysis. Yet, the assessment of the accountability mechanisms in this study shows that, by excluding radical and deeper attempts of citizen oversight, intelligence might put a threshold over itself. Firstly, intelligence enhances surveillance and the management of populations by exceptionality procedures. Secondly, the attempts

to improve legitimacy are limited to the previous forms of accountability that tend to be indirect, contingent, or incomplete. Thirdly, intelligence excludes the right to subvert the sociopolitical order by legitimate means (as in the notion of negative freedom explained in Chapter 1). Also, there is no real incorporation of citizen groups in the formulation and evaluation of security and intelligence policies. Hence, intelligence produces a double exclusion of people: from the attempts to oversee their rulers, and from a problematic categorization in case they are watched as potential threats against the sociopolitical order. The double exclusion, in turn, opens a legitimacy gap between the authority of the order and the populations who are governed. Also, the legitimacy gap creates the conditions for the sustainment of the order at the expanse of illegitimacy levels attached to those who watch and govern in the name of security. Fourthly, considering a historical perspective, in moments of crises, either this gap is eventually filled with radical but legitimate attempts of renovation that challenge politics in a broad sense, or the short circuit between legitimacy and authority could produce illegitimate forms of resistance (even violent in extreme cases) as well as illegitimate forms of counter-resistance by the governing institutions. The lines above are worthy of consideration as no sociopolitical order endures forever. The transition between different orders might take decades or centuries. Yet, authority should be considered as contingent, unstable, and something that must be bargained all the time, instead of a constant power that must be preserved at any cost.

In light of that, maintaining the door closed to critical approaches and to the incorporation of dissonant voices in intelligence policies would disallow the opportunity to expand this field beyond prescriptions oriented to support high-decision makers. That is, it would prevent to analyze this governmentality technique beyond its internal principles and performance to restricted audiences. It also would prevent to expand intelligence to the deconstruction and recreation of new guidelines related to the very act of governing. In addition, "while the role of intelligence is to reduce uncertainty for decision-makers, a role of intelligence scholars is to highlight uncertainty, that is, open up possibilities for ethical reflection and deliberation that conventional wisdom, institutional inertia, and mainstream research have closed off" (Bean, 2013, p. 495).

Critical approaches are also important to analyze resistance to surveillance, including intelligence. Resistance, in radical terms, is not only a task from people that hide something or criminals. Resistance in this realm, as expressed in the theoretical framework, does not consist of the final victory of the watched people over the watchers. It consists of the continuous forms to restrain, redefine and transform the surveillance assemblage including attempts to improve intelligence by institutional channels but also by radical dimensions. This recalls an old expression by Hanna Arendt: it is essential to create space for civil disobedience (in the sense of dissidence and continuous reinvention) in the actions of our public

institutions. We will return to these possibilities analyzing the civic agency in the next chapter and in the last Part 4.

Part 2 consisted of Chapters 3 and 4. In Chapter 3, we analyzed intelligence concepts and studies. Moreover, we analyzed the accountability mechanisms that have emerged to restrain intelligence agencies from authoritarian legacies in the 1970s to the present time. We have explored internal controls, legislative control, judicial control, international oversight, and the media and civil society role. To base the analysis, the chapter used primary sources from the parliaments, data from the media, jurisdiction and laws, and specific literature in each country. By the study of these mechanisms, accountability has been mainly promoted through answerability. This principle consists of demanding answers or to clarify "wrongdoing", negligence or inefficiency to the eyes of accountable actors. As these terms are difficult to be measured in a secret domain, the combination of legislators, courts, the media and other players was important to promote even some levels of enforcement and transparency. In terms of responsibility, the duties and missions expected by intelligence, this principle has been especially promoted by internal controls from the Executive itself as it has the last prerogative to assume modifications in intelligence policies.

In Chapter 4, we returned to the concept and theory of surveillance to connect the main findings in Chapter 3. The points of connection are regarded to surveillance metaphors such as the panoptic and rhizomatic assemblage in intelligence, the management of subject and populations, and new forms of resistance and legitimacy. Accountability here depends on contingent variables, a convergence of actors, and a network of governance to overcome transparency challenges and the exceptional characteristics of intelligence. However, the accountability mechanisms have limited potential to preserve individuals' autonomy and recalibrate the asymmetry of power between watchers from the state and the watched populations. Legally speaking, intelligence is not supposed to spy on their citizens (even if we mentioned several occasions when this could have happened). Yet, when intelligence is analyzed through the lens of surveillance, it becomes clear that it also constitutes a governmentality tool and a biopolitics regulator. Thus, it is essential to think of new accountability mechanisms, especially by the role of civil society to reach greater levels of legitimacy. In that sense, we expressed that intelligence can be reviewed if one considers legitimate resistance and dissidence. A priori, intelligence and these terms seem to collide or constitute an aporia. Yet, their relationship can open new forms to understand the limits of intelligence but also the very forms of power in contemporary societies.

The next Part 3 analyzes accountability mechanisms in the second surveillance realm: the governance of personal data. The examination of both intelligence and personal data realms is essential to expand the frame of accountability and reach the study objectives, as well as to depict more interactions and actors that hinge on surveillance. Lastly, Part 4 will revisit the notions of resistance and accountability, from reformative to radical principles. This part redefines accountability as a relationship between authority and legitimacy and explores new mechanisms to restrain power in surveillance and politics in a broad sense.

PART 3

Chapter 5. Accountability in the realm of personal data

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.
Bruce Schneier

During the 1960s, exceptional institutions of surveillance, as the Spanish and Brazilian intelligence services, were created to "dominate" hearts and minds by fear. However, in recent times, these services no longer centralize many of the dispositives for surveillance. There are many domains beyond intelligence in which surveillance can be done on a larger scale and with more efficiency than in the 1960s. Since the 1990s, one of those domains is the governance of personal data on the Internet between public and private organizations, both national and international. In this governance, people can be attracted and be watched by the surveillance dispositives by soft means. In simple terms, attraction can be more efficient than fear to watch habits from people.

Because of that, the migration of a wide range of social, professional, and personal communication into digital and commercial platforms has raised new questions that affect individual autonomy: what level of disclose about the collection of personal data is compatible with privacy safeguards? What types of accountability mechanisms should be placed on the use of personal data? These questions are added to previous ones that were not completely answered in the past: what levels of controls must be constructed against abuse and deviation of power in sociotechnical infrastructures? What level of tyranny is hidden in friendly and open surveillance tools? All of those questions are of vital importance to understand the past and the future of our societies. They matter because they help to reconstruct lessons learned from dictatorial experiences and to improve power legitimacy in the times to come. As explained in the theoretical discussion, information from individuals can be sorted, fragmented, classified, extracted, and recombined in different ways. Something done in one context can be relevant in one domain but intolerable in another. Thus, we will address different actors to analyze the management of personal data. First, we will reconsider some notions of personal data (section 5.0). Then, we examine the accountability mechanisms in this realm considering three domains: state regulations (section 5.1), market strategies (section 5.2), and civic agency (section 5.3).

5.0. Personal data

After the triumph of the Internet in the 1990s, this technology was considered as a redeemer, as the reinvention of democracy; a huge leap towards the improvement of individual autonomy (Hiltz and Turoff, 1978; European Information Society Forum Report, 1999; Blaug, 2002). However, many authors have been cautious and less optimistic about the Internet. Instead, they have denounced the digital exclusion and the cooptation of democratic potentials by stronger and hegemonic players (Margolis and Resnick, 2000; Noam, 2002; Castells, 2013). In recent decades, for example, social networks that were initially celebrated as democratic tools became targets of closed regimes as in the case of the Arab Spring in 2013. The same year, after the Snowden revelations, it became clear that, despite the variety of interests and clashes, some states and large corporations can manage information in a powerful manner because they also have a consolidated power position in the offline world. Therefore, while we reject utopian and dystopian simplifications that followed the Internet triumph, it does not mean that the cyberspace is disconnected from traditional forms of power. In that sense, we adopt a holistic approach which is also cautious to understand how the content of the Internet is managed, especially in the case of personal data.

Personal data is a piece of information related to an individual or a physical person. Once shared voluntarily or extracted from an individual, that piece must be considered as a strategic component of one person instead of his/her ontological image or essence. Personal information can be interpreted by philosophical terms (as the abstraction and the identification of the "being"), by technical means (such as analogical registers, digital codes, and fragmented information from a data subject), judicial means (for example, separating the owner and the processor of this information, and creating rights for consent and deletion of personal data). Traditionally, unique personal information served to create a core identity based on biological ancestry and family. Throughout history, in societies with little geographical or social mobility, people were rooted in local networks like family, village, community bonds, and social position. People used to be identified in personal terms (name, physical aspect, family) or through smaller information networks (Church, school, workplace). Thus, the information of those persons was attached to the presence of the consciousness of that same person. In societies with increased mobility associated with urbanization and industrialization, core identity came related to biopolitics –the administration and power over physical bodies- that relied upon different individuals' information such as name, birth certificate, national identity, credit cards, and so on.

Nowadays, with the expansion of biopolitics and surveillance tools, we see individualization efforts based on DNA, voice, retina, facial geometry, and other

cyber/biological approximations that are even more detached from the person itself. That is, personal data can be processed independently and can constitute data doubles, the re-presentation of the persons and identities in an overall sense. Personal data became strategic parts to be recognized by external gazes to create a provisional identity and to validate individuality. For example, card numbers, photography, and other tools emulate names and bodies, becoming even more important than bodies to validate our lives in the face of institutions, markets, and to grant mobility (social and geographical).

At the same time, personal data is always a process of recombination of previous data (in the sense that even our biological bodies are recipients of data). This recombination can be oriented to certain goals and expectations. Yet, sometimes, the procedures to recombine them escape from our control. In that sense, Johnson & Regan (2014) use the "house of mirrors" metaphor to describe personal data recombination. As when a person enters in a house of mirrors and sees his/her image distorted due to the movement and the position of the mirrors, according to those scholars, individuals information is sorted, bounced and rendered by socio-technical tools in many ways and with different purposes (campaign financing, secure flights, search engines, social networks, online advertising and so on). Thus, not all types of personal information are used in the same way and have the same importance for watchers and the watched. On the other hand, Gary Marx (2004), for example, offers a typology to describe the kinds of personal information most commonly related to data subjects (individual identification, geographical/locational, networks and relationships, behavior and beliefs, media references, etc. See Chapter 1). Other scholars prefer to use the term digital persona,

> In Jungian psychology, the anima is the inner personality, turned toward the unconscious, and the persona is the public personality that is presented to the world. The persona that Jung knew was based on physical appearance and behavior. With the increased data intensity of the second half of the twentieth century, Jung's persona has been supplemented, and to some extent even replaced, by the summation of the data available about an individual. The digital persona is a construct, i.e., a rich cluster of interrelated concepts and implications. […] The digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual (Clarke, 1994, p. 78).

In societies where everything can be measured, compared, and rendered in a culture of performativity (Lyotard in Peters, 2004), it becomes natural that personal data constitutes itself as the main fuel to supply surveillance networks nowadays. The encounter between data and surveillance is called Dataveillance, which means the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons (Clarke,

1988). Dataveillance differs from physical and old electronic surveillance (like the political vigilance of populations during the 1960s and 1970s in our cases of study) and involves monitoring not only individuals but their data. Monitoring is virtual and almost omnipresent. I requires indirect contact since individuals are surrounded by ubiquitous electronic devices, and construct their personality also through online interactions. Data performance is immediate and contingent, rather than fixed or attached only to one purpose. Hence, two classes need to be distinguished: Personal dataveillance, in which a previously identified person is monitored, generally for a specific reason; and mass dataveillance, in which groups of people are monitored for different purposes, generally to identify potential targets of interest to the surveillance organization (Van Dijck, 2014).

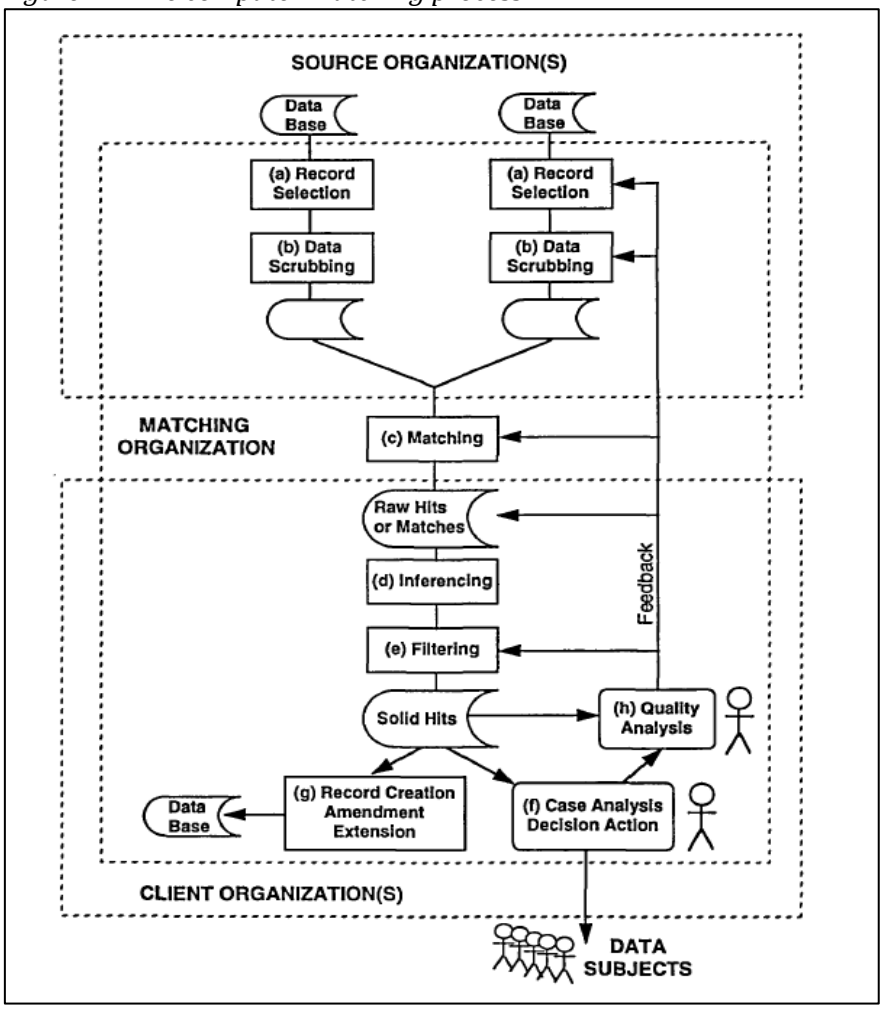
Since the 1990s, the Internet implied in the rise of dataveillance, and we focus in this kind of surveillance as it is closely attached to personal data. We do not focus directly on CCTV´s, biological records, image, face and voice monitoring unless they are stored in personal databases on the Internet and used for surveillance purposes. It means, cameras on the streets can record our image, but unless they are not processed and stored as personal databases and shared in broader online surveillance networks, in our view, they barely constitute sources for dataveillance. The borderline between those topics is hard to be established as almost every content produced for surveillance, at least electronically, can be converted into sources for dataveillance on the Internet. Especially in the case of mass dataveillance to watch large populations.

Dataveillance matters because, for the individuals, it represents the simulation of their identity, and so of their conditions of everyday politics to live in society. A bias or deliberate alteration in surveillance mechanisms can foster the suppression of opportunities, enhance incoherent representations, and even define material conditions for a living (like being arrested or obtain health insurance). In that sense, if the individual has some degree of control over her data, she is also influenced by the digital data (or digital persona) created by others (especially by data processors). And since surveillance is about how to use the gaze and how the gaze defines us, each person maintains formal and informal relations to constitute her individuality and to be observed depending on the context and gazes that are subjected to. The data intensity of contemporary business and government administration results in vast quantities of data being captured and maintained, allowing considerable opportunity to build formal data doubles or “dividuals” rather than individuals, as stated by Deleuze (1995) in his idea of social control.

When (in)dividuals use or produce data, they can act as passive or active subjects. Passive subject means that the representation of the data double or “dividual” is projected or imposed over the individual. In that sense, the individual can be deemed as a source and producer of digital content. On the other hand, active subject means that individuals can react to those projections, and exercise

some level of resistance to the representation of data. "It enables individuals to implement filters around themselves, whereby they can cope with the increasing bombardment of data in the networked world" (Clarke, 1994, p. 78). These filters are not fixed barriers, because individuals can self-modify them according to their preferences or feedback obtained by other people and data processors; we will address the active forms of resistance from data subjects in section 5.3 of this Chapter.

Figure 13: The computer matching process



Source: Clarke (1994, p. 85)

Every process related to dataveillance starts from a basic step: the ability to collect data, and the capacity to process and create additional valuable data. The process and refinement of data, as in the sense of raw oil being converted into new valuable materials, works thanks to matching and crossing previous information in computers and automated machines. This process raised in the 70s and became a normalized practice in bureaucracies and companies nowadays. Since the 80s concerns about privacy were raised by computing matching (Shattuck, 1984). If in those times the term "algorithm" was barely understood, today it appears as a

constant word in media, films, engineering, games, governance, climatology, and almost every social domain. Data matching could be done in two ways: a) by identifying or searching common identifiers among the bulky data; b) by looking for correlations among different identifiers in data. One example of the common identifier is the act of creating profiles or categories of suspicion crossing and matching data. This can be obtained from seeking correlations and creating patterns as in the case of consuming, voting preferences, health and behavior habits, and so on. The figure above shows how computing matching works from source to client organizations.

The figure indicates source organizations as those that contain data from individuals, like register, affiliation, identification, etc. Source organizations record and scrub data according to their internal needs and demands. Local police agencies, for example, can establish databases for suspects, offenders, and create criminal records. A hospital and even the education office can create databases for patients and students. In the next step, matching organization not only scrub data, but also use computing inferences, filtering, and create "solid hits" or identifiers that enable add valued data for decision making (used to offer services to data subjects). Matching organizations "deliver" those products to client organizations. Matching organizations can produce new databases, and formulate quality analysis that in turn demand more data from source organizations restarting the circle. It is important to notice that those roles can be found in one institution. Moreover, the same institution can have roles in different steps of the cycle. For example, the police agency of our previous example can be a client organization from a third entity (i.e. private firms, intelligence agencies, or even other enforcement institutions) who matched data from the sources and databases from the police.

Matching organizations, in general, require technical means and the capacity to process huge amounts of information. As matching algorithms and data clients work at an accelerated pace, huge corporations of technology dominate this field. In the "western world", Google, Apple, Facebook, Amazon, are 'source' and 'matching' organizations that offer aggregated data for clients, from marketing and consuming companies to law enforcement agencies. Their products, in turn, address data subjects who restart the cycle supplying the 'source' organizations with new data. In this view, most of the use of data consists of gathering, processing, and delivering data in similar ways commodities or natural resources are transformed into valuable products and services. Yet, the automated gathering and matching of bulky data will depend on the context or social domain in which data is processed. Thus, we will analyze briefly the governance of personal data and accountability in specific domains. Those domains include the state, the market, and society. To be precise, we address 1) state regulations, 2) market strategies, and 3) civic agency.

5.1. State regulations

In this section, we examine the main answers formulated by states to regulate the management of personal data. The first data rules were enhanced in the 1990s, after many judicial clashes and as an effort to institutionalize data protection authorities in Spain. Meanwhile, the Brazilian case presented partial regulations as the digital Constitution (the Internet Civil Framework) in the last decade. Yet, only in 2018, both countries introduced deeper and new regulatory mechanisms to oversee data rights and uses. In the following pages, we analyze the evolution, rules, and scopes for personal data protection in Spain and Brazil.

5.1.a. Personal data protection in Spain

It is important to notice that personal data protection in Spain was updated according to the norms and rules established in the process of integration of the European Union (EU). At the European level, Article 8 of the Charter of Fundamental Rights of the European Union (CFREU) recognized the protection of personal data as an essential right:

> Everyone has the right to protection of personal data, such data must be processed fairly for specified purposes and based on the consent of the person evolved or for some other legitimate basis provided by law, and everyone has the right to access the data collected relating to him/her and to get it corrected. (…) compliance with these rules shall be subject to control by an independent authority (Art. 8, CFREU).

Moreover, the European Parliament has produced several legislations on this subject. It is of importance the Directive 95/46/EC to protect the rights of individuals when it comes to processing and transferring personal data. Other milestones were the Directive 2002/58/EC to protect privacy and data in electronic communications; the Regulation (EC) 45/2001, which allowed the creation of the "European Data Protection Supervisor" (EDPS) as the authority (consultation and cooperation) responsible for ensuring that independent institutions and organizations inside the Union perform theirs obligations regarding data protection. The Decision 2008/977 (Council on Justice and Interior Affairs) also regulated the protection of personal data processed in the framework of police and judicial cooperation as well as in the criminal area. This Decision regulated data protection in accordance with the previous "third pillar" of the Union and it is only applied to police and judicial data exchanges between the Member States, authorities, and systems of the UE (without the direct inclusion of national databases). In the "Area of Freedom, Security and Justice" (AFSJ) –which is

the front of the EU regarding security and surveillance - the main systems among the Member States to collect personal data are the Schengen Information System (SIS), the Customs Information System (SIA), the Information Visas System (VIS) and the European Police Agency or EUROPOL. Those systems are covered by the above-mentioned norms. For example, as of 1 May 2017, the European Data Protection Supervisor (EDPS) has been responsible for supervising the Europol data protection measures.[75]

After the advent of the Internet and the expansion of electronic communication to the public since the 1990s, both public and private institutions, at Spanish and European levels, deployed measures to protect privacy and manage the protection of personal data. Information such as personal data should not serve for disproportional measures and deregulated goals in the hands of state/economic powers. In that sense, personal data protection is a new form of accountability involving both responsibility, answerability, and enforcement. On the one hand, data protection rules are concerned about the misuse of data in surveillance assemblages that monitor "all aspects" of our digital lives. On the other hand, many citizens could think that been exposed and see the others are entailed by a space of great freedom and transparency. Yet, it is essential to remind that transparency could be produced in one side (at the bottom of society, in the side of "normal citizens"), instead of being promoted matters of national security and exceptional sovereign powers (at the "top" of society). That is, transparency can be fostered in the side of the citizen (the watched), and neglected or ignored in the side of strong data processors from state/market (the watchers).

In that sense, the metaphor of "slides of visibility" from Bakir & McStay (2015) is very useful. It implies in a slider buffer to set the levels of transparency in the sides of the watched or watcher in three categories: Liberal transparency, total transparency, and imposed transparency. The first category is related to the liberal trend of checks and balances and the essential task of turn accountable the "powerful". It seeks to oversee the watchers and can be exemplified by the mechanisms of accountability from state and justice. It also considers the individual as a judicial person of rights to be protected in several contexts. Liberal transparency means visibility especially to oversee governments. In this category, society tends to win when political decisions are taken in transparent conditions, discarding lies and secrets.

Total transparency, the second category, is a general proposition with no foreseen effects. It entails transparency both in the sides of watchers and watched. In this category, if top organizations and governments ought to be transparent, the same logic should be applied to their citizens and people (Bakir & McStay, 2015). For example, some security officials and intelligence analysts might support this

[75] European Data Protection Supervisor. 2016, May 19. 'New Regulation boosts the roles of EDPS and Europol'. Press release, retrieved from: https://edps.europa.eu/node/3336 in 12/01/2019.

vision in order to create transparent citizens. They might repeat the traditional "nothing to fear if there is nothing to hide", "privacy is dead", or "more security requires greater sacrifices of privacy" because "we need to watch the bad guys". At this point in the text, we hope that those mottos are put into question by the reader. In the theoretical framework, we have shown why power will always carry secrets and the illusion of total transparency. Yet, total transparency could be radical, indicating a scenario where both watchers and watched are more transparent to each other. This scenario can be related to the term "sousveillance", which means that the bottom of society, the normal citizens, are mutually transparent to each other (Mann, Nolan, & Wellman, 2003). In a positive approach, not only they show and uncover their lives as in the synoptic metaphor, but they also can take care of each other by surveilling their peers, as in the case of neighborhood vigilantes applied to restrain criminal offenses. At the same time, the bottom can watch the top, the traditional watchers, revealing their actions, and monitoring their activities. Then, sousveillance would be the opposite direction of the gaze embedded in surveillance, a vision from below to above and to everywhere.

Finally, obligated transparency, the third category, consists of a scenario where citizens from the bottom of society are "obligated" to be transparent whereas the top players, the surveyors, are hidden. In other terms, the latter imposes, by implicit or direct power, that citizens expose themselves without knowledge or consent. This is the case, for example, of intrusive mass surveillance and the disproportional monitoring of targets. After the Snowden revelations, some scholars mentioned that forced transparency is the current situation of societies nowadays (Bakir & McStay, 2015). However, we need to avoid oversimplifications and see the potential of accountability when it comes to gather and process data. In that sense, the fact that the regulations to protect data enforce direct access, rectification, consent, and opposition to surveillance (at least in certain scopes, even if they do not encompass totally security and mass surveillance), shows that liberal transparency supporters and voices against forced transparency could be combined to turn surveyors more accountable.

In that effort, one problem of personal data protection rules is that they are jeopardized by a sort of generic narrative about responsibility and values that are in vogue instead of a real internalization of the same principles by institutions and persons. This statement can be attested when we appreciate the evolution of the right to data protection in the European legal systems. In this case, European countries began by recognizing the right to data protection (privacy, dignity) as a general principle of Common Law, and incorporated it to the jurisprudence of the "European Court of Human Rights" (ECHR) as well as of the "Court of Justice of the European Union" (CJEU). That is, to check the "proportionality" and justification of the cases that could interfere with those rights, the jurisprudence is supposed to be a mechanism to supervise and, theoretically, to enforce and turn accountable those

activities that process personal data (including organizations from the administration and market). The Jurisprudence also tried to reinforce the roles played by data protection Agencies both at national and European levels. Notwithstanding, accountability efforts depended more on critical junctures (leaks, scandals, disproportional security measures) than in defining specific roles and mechanisms for data protection Agencies. The protection of personal data within judicial scopes in the European context traditionally has been very incipient (Sphere Ramiro, 2011).

For instance, the thresholds to accountability were attested in cases such as the "Österreichischer Rundfunk" in 2003. In this case, the CJEU considered that national government tracked personal incomes and bank accounts, thus, they interfered with the protection of personal data. However, the CJEU decided that gathering this kind of data could be justified when it is appropriate for the "good management of public funds" (Piñar Mañas, 2003, p. 64). Though, the definition of "good" is unclear and unpredictable.

Since 2012, in cases labeled as "Digital Rights Ireland" the CJEU was persuaded to take legal actions over electronic data retentions provided by the "Criminal Justice Act" (Terrorist Offences) of 2005. In addition, the Court was swayed to decide about personal data transfers to third countries like the United States via private companies like Facebook. The CJEU considered the Act invalid and claimed the strengthening of the European standards for privacy and personal data protection. According to Pascual (2014, p. 953), despite the Digital Rights Ireland case, the delay of this decision can be explained by the "reluctance of the Courts to cooperate" in this issue.

Another attempt to turn personal data processors more accountable was enhanced when "Google Spain" and the Spanish DPA (AEPD) clashed about the so-called "right to be forgotten" in 2010. In this case, the AEPD ordered Google to de-index pages that affected the privacy and dignity of a lawyer contractor. In the AEPD's view, it was legal to publish private content from that person in a newspaper because it was a matter of press freedom to express content. However, there was a violation of privacy laws when Google helped other people to find personal content on the Internet. In that sense, the AEPD claimed that the search engine company is also responsible for processing personal data even when the content is legally public. In 2014, Google appealed the AEPD decision in the Court of Justice (CJEU) but this court affirmed the existence of a right to have personal data deleted if request by the data subject.

A different example happened in 2017 when the European Commission for Antitrust practices fined Google €2.42 billion for abusing its dominant position as a

searching engine to promote Google Shopping.[76] Consequently, Google needed to modify its search engine algorithms that combine personal data preferences with online market advertising. In particular, the decision required Google to treat rival shopping services and its service equally, respecting users' liberty to choose products and services on the Web. However, it has been argued that competition law, even modified from the current antitrust approach, is not able to disable this kind of practice only by economic measures. For instance, this effort has to be part of a multi-regime response involving regulation and consumer law (Daly, 2017). In short, a multidimensional approach to regulate economic giant data processors is necessary and urgent as suggested by the European Data Protection Supervisor (EDPS), which expressed the necessity to deploy coherent enforcement of fundamental rights in the age of big data.

The European Parliament (EP), in regard to fundamental rights implications of big data for privacy, data protection, non-discrimination, security, and law enforcement, has also made a call for "closer cooperation and coherence between different regulators" endorsing "the establishment and further development of the Digital Clearing House as a voluntary network of enforcement bodies" to "deepen the synergies and the safeguarding of the rights and interests of individuals."[77]

In addition, the Court of Justice of the European Union (CJEU) has also judged issues that affect personal data. In October 2020, The CJEU expressed a series of decisions (C-623/17, Privacy International, C-511/18, La Quadrature du Net and others, C-512/18, French Data Network and others, and C-520/18, Order of French-speaking and German-speaking lawyers from Belgium and others). By these decisions, European Union law prevents State Members from requiring an electronic communications provider to conduct general and indiscriminate transmission or retention of data, such as traffic and location, to defend national security and prevent crime. This affects not only intelligence but also electronic and telecommunication companies that handle data.

For those reasons, we must underscore that a set of external controls has been deployed, especially through legal frameworks and in some cases by enforcement dimensions. Yet, there are many fronts on this field that must be promoted, specifically by "third dimension" or international accountability efforts (see section 3.7).

---

[76] *European Commission*. 2017, June 27. 'Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to its own comparison shopping service'. MEMO/17/1785. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 in 12/03/2019.

[77] *European Parliament*. 2017, February 20. 'Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement. (2016/2225(INI))'. Retrieved from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0044+0+DOC+XML+V0//EN in 12/04/2019

To complement those fronts, the “General Data Protection Regulation” (GDPR) enacted by the European Union in 2016 updated the previous rules in this field, such as Directive 95/46/EC, and can be considered as the main legal milestone developed so far.[78]

The improvement of the legal framework by the GDPR was also a common answer to the following points: a) the lack of distinction and the ambiguous definition of "personal data" and its "protection" in the sense that data relies on logic criteria to be stored and related to individuals. That is, despite the fragmentation and advanced tools to anonymize data, it should be processed within clear lines and with consent from the data subject; and b) the need to define new standards of "transparency", "responsibility" and "accountability" in several social practices related to the use of personal data.

Approved in 2016, the GPDR is valid if a data controller or company (organizations that collect data from EU residents) or processor (organizations that process data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based on the EU. According to the European Commission, “information relating to an individual such as a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address” are some targets for the regulation. The GDPR affects government, market, and social data processes but its terms do not apply when personal data is handled for national security purposes. Hence, state surveillance and anti-terrorism intelligence international cooperation remain as “untouchable” zones that need specific legislation in each Member State of the EU (see Chapter 3, section 7).

It is important to notice that the GDPR demands data controllers to implement security measures also in accordance with market strategies for data protection. The legal reform explicitly mentions the term “Privacy by Design and by Default” (Article 25) requiring data protection procedures since the design of business systems to the elaboration of products and services. Moreover, Data Protection Impact Assessments (Article 35) have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation protocols are mandatory in case of high risks to personal data. In this case, prior approval of the Data Protection Authority (DPA) must be obtained by the data processor. Besides, Data Protection Officers (Articles 37–39) must be hired to ensure compliance with the GDPR in each company. In addition, Article 47 stipulates DPA as an independent supervisory authority that oversees and exercises his/her power in accordance with this Regulation. Articles 35, 37, 38, and

[78] *European Parliament and Council*. 2016, April 27. ‘Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)’. Legislative acts. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 in 12/05/2019.

39 are especially linked with the market principles, such as corporate accountability. Therefore, digital management in market spheres and data protection regulations have reached greater levels of convergence. The GDPR encourages a reform that facilitates digital market practices and information exchanges. Besides, it privileges accountability functionality dimensions over institutional lines as a way to overcome the thresholds of the previous Directive 95/46/EC. For instance, private organizations need to incorporate internal oversight accountability principles (such as horizontal audits and risk assessment) and personal data files must be processed according to the scope and range of each company. There is no obligation to maintain data lists in a DPA. However, data breaches and security deficits must be communicated immediately to the DPA (Article 33). In that sense, if the previous regulation was more hierarchical or vertical and bureaucratic oriented, the GDPR adopts a flexible control, promoting self-regulation and self-supervision in each company. This control should be ensured by Data Protection Officers all the time and by the DPA authorities in exceptional or sensitive cases.

Despite the devolution of power to implement "good" practices from DPAs to each company, the GDPR creates new challenges. Firstly, the GDPR requires comprehensive changes to business companies that had not implemented a comparable level of privacy before the regulation (especially non-European companies handling EU personal data). Secondly, Article 83 stipulates general conditions for imposing administrative fines according to the nature, gravity, the number of data subjects affected, and the level of damage suffered. Such fines are clear points that support enforcement accountability, avoiding a toothless regulation, and binding companies to adopt "privacy by default" measures. Since the DPAs cannot oversee the bulky information collected by data processors, it is reasonable to complement institutional roles with a regulation that enhances capillarity to penetrate organizational market functionalities in order to improve accountability – especially to protect the privacy and individual autonomy.

In the case of Spain, if we look at the transposition of the European rules, one can see that Personal data protection was not mentioned in the Spanish Constitution of 1975. It only appeared as a fundamental right recognized by judicial terms almost two decades later. The first milestone on this issue, the Act (STC) 253/1993 (updated by the Royal Decree 1720/2007) expressed personal data as a fundamental right both in negative and positive rights. The STC 253/1993 established several points to define and implement administrative mechanisms to protect citizens' data. By Article 3, personal data was defined as the information that could be associated with a physical person. In that sense, it includes all types of data regardless of the form, presentation, or media (voice, images, videos, fingerprints, genetic data, etc.). Whereas the same Article establishes file systems to store personal data, a controversial point emerged since the data could be mixed or fragmented, annulling the logic of a "sorted and

structured information" (alphabetical, numerical, the order of arrival, code number, etc.) of the Article. In addition, the Act established a public or private organization as responsible to store and protect data: the data controller. Controllers were of importance for the A.R.C.O. rights and demands associated to data protection (access, rectification, cancellation, and opposition) because they needed to communicate periodically to specific providers or intermediaries (data processors), which in turn can ensure access to data flows and work with this information after the consent of users (Articles10-15). Another milestone was the creation of the "Spanish Personal Data Protection Agency" (Agencia Española de Protección de Datos - AEPD) as the public authority responsible to implement administrative sanctions and to control public and private file systems (both analogical and digital) in the Spanish territory. In that model, data controllers and processors were demanded to register their lists (databases) in the AEPD, showing the nature and the sensitivity of data they processed. Considering the constitutional pertinence of those rights, at the beginning of the century, the Supreme Court Acts (STCs 290/2000 and 292/2000) reassured the compatibility of personal data protection with constitutional backgrounds.

In terms of accountability, an important institutional design was the fact that the Agency (AEPD) became administratively statutory and was constituted as an independent organization. Yet, its financial autonomy and presidency indication are verified and assessed by the Ministry of Justice. At the same time, the AEPD function is to receive citizen's petitions on data protection to execute the A.R.C.O. rights related to subjects (access, rectification, cancellation, and opposition). In addition, the Agency was established to demand responsibility and external "answerability" of personal data systems and processors, including those systems stored by police and security services (Article 22, Organic Law 254/1993). On the other hand, this control is not implemented when personal data issues hinder the fulfillment functions of public authorities, and when "National Defense, Public Safety, criminal and administrative prosecutions could be affected" (Article 23-4, Organic Law 254/1993). As this proceeds, the answers given by the legal framework were hampered in cases when personal data is confronted against security issues (Guasch Portas, Fuensanta, & Ramón, 2015, p. 417). Besides, accountability within the AEPD scope is limited due to its national jurisdiction and administrative range. Thus, other agencies on personal data were created inside and outside the country, such as the Basque and Catalonian Personal Data Agencies (Spain could be labeled as a quasi-federal state), as well as the "European Supervisor", whose tasks include, for example, personal data transfers and maintenance of data processor lists in the European Union.

More recently, the GDPR aimed to be transposed to national regulations in State Members. In Spain, Law 3/2018, of December 5, on the Protection of

Personal Data and Guarantee of Digital Rights (LOPDGDD)[79] was approved to embody the GPPR in a comprehensive manner. Yet, it still needs to be completely transposed. The EU has even sued Spain for not embodying and implement the complete transposition of the GDPR fundamental framework.

LOPDGDD main modifications in relation to the previous Spanish rules are as follows:

- It is necessary to keep records regarding the treatment of data (art. 4-10, art. 31)
- Not every data is personal or has the same importance. Thus, it is important to determine the legitimizing base for data treatment. The Spanish law follows the European Regulation in six bases: Consent of the interested party, necessary for a contract, fulfillment of the legal obligation, necessary for mission in the public interest, the legitimate interest of the controller or necessary to protect vital interests of the interested party (art. 6-10).
- The need to comply with the principles - obligations – from the European Regulation: data minimization, limitation of purpose, confidentiality and integrity, legality, loyalty and transparency, time limits of conservation, and accuracy (Title V, art. 28-32).
- Modification in the maintenance and in the process of data. From file system records attached to the AEPD (Spanish DPA) to a flexible self-supervision logic in which each processor elaborate continuously reports the treatment of data.
- The former A.R.C.O. rights are extended including the right to be forgotten (data deletion), and right to portability (from one data processor to another one in order to deliver services) (Title III, art. 12-18).
- Data processors need to improve the technical staff and the security of information systems. By the new law, every data processor needs to hire data protection officers (art. 34-37).
- In case of severe damage and risks to data, they should be communicated immediately to the DPA (Title VIII, articles 63-69). Besides the internal audits and traditional reports, data processors also need to conduct risk assessment impacts in their systems (art. 51-54).
- Comply with the principle of accountability: data processors must redact and track all the actions taken in order to comply (by proactive manners) with the previous articles (Title IX, articles 70-78).
- Creation of an administrative fine regime from €900 to 600,000, or in case of companies, from €10-20 million or 2 to 4% of the annual turnover revenue budget.

[79] Jefatura del Estado. 2018, December 6. 'Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales'. *Boletín Oficial del Estado* (BOE). Retrieved from: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf in 12/07/2019

There is no doubt that the European regulation and the Spanish LOPDGDD aim to respond to the enormous impact of Information Technology in the political, social, economic, and leisure aspects of life. Besides, the regulation aims to answer to new realities that were not faced back in 1992, when the first legislation was issued, and in 1999, when comprehensive Spanish data protection rules were activated. Nowadays, in times of social networks, cloud computing, and big data, legal measures need to catch up with technological changes and uses. This is not a race against technology, but a continuous legal development that needs to tackle something that is not fully controllable in the strict sense. However, considering the continuous normative reforms and the technological challenges, important points can be mentioned in the legal effort to protect data.

The first one is related to the still differentiation between public and private spaces (even in the cybernetic world or in terms of the scale of privacy). For example, LOPDGDD Article 22 focused on treatments of data for video surveillance purposes makes a clear distinction between public spaces and private houses and facilities. The article mention that data processors may obtain videos and images in order to preserve the safety of persons and property, as well as their facilities. But those images can only be obtained in public spaces and domains. The images cannot be extracted from the individual or familiar spaces (homes, zones of private transit, etc.). Then, as some spaces are essentially private, the public necessity of surveilling must be notified to users and the images should be captured respecting the principle of proportionality and durability (deletion of data).

In case of processing personal data from images and sounds obtained through the use of cameras and recorders by the Security Forces (Police), by Correctional Guards and Transit Officials, surveillance shall be governed by the Directive (EU) 2016/680. According to this Directive, the processing of images for those purposes is allowed when the treatment is intended for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, including protection and prevention against threats against public safety. Similar logic applies in the case of labor surveillance (monitoring of data in working places), where the privacy of workers should be respected (Article 89). In that sense, interference with privacy should be motivated by public necessity and reasons (i.e., security, prosecution of offenses, investigation, etc.). As in the case of judicial control of intelligence, every right can have exceptions but those exceptions need to be justified and executed within accountability principles (see Chapter 3, section 6).

Moreover, the protection of personal data is an important accountability mechanism to mitigate the pathological side of surveillance when it comes to process and use data for unforeseen purposes and opaque biopolitics (personal data management is one reformulation and extension of biopolitics, as expressed

in Chapter 2). To do so, Article 22 of the LOPDGDD defines that responsibility for the treatment shall take into account the following risks and situations:

> a) When the treatment could generate situations of discrimination, usurpation of identity or fraud, financial losses, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of anonymization or any other economic, moral or significant social damage for those affected.
>
> b) When the treatment could deprive those affected to exercise their rights and freedoms, or when they are prevented from exercising control over their personal data.
>
> c) When the treatment involves an evaluation of personal aspects in order to create or use personal profiles, in particular by analyzing or predicting aspects related to performance at work, economic situation, health, personal preferences or interests, reliability or behavior, financial solvency, location or movements.
>
> d) When the data processing affects groups in situations of special vulnerability and, in particular, minors and persons with disabilities.
>
> e) When there is a massive treatment that involves a large number of affected persons, or the collection of large amounts of personal data.
>
> f) When personal data is transferred, on a regular base, to third States or international organizations that lack an adequate level of protection of personal data.

The points above are examples that seek to preserve a certain level of autonomy in the side of the data subject. They can be interpreted as legal accountable measures that reinforce the first objective of this research. That is, personal data matter to preserve a certain degree of identity, liberty, and sovereignty of data subjects, especially when they face surveillance mechanisms and data processors with a huge capacity to alter data (from banal commercial purposes to the production of surplus commodities and to distinct forms of categorization that might reinforce discrimination, exclusion, and redefine social positions) and expand the asymmetry of power between individuals in the social stratifications and between data subjects and data processors.

The above points also show that the LOPDGDD aims to promote accountability by responsibility since it mentions that there must be persons who are responsible for the process of data. “The responsible person for the treatment […] shall contact data subjects regarding their rights and violations to this rule, even when there is a contract or legal act with the content set out in Article 28.3 of Regulation (EU) 2016/679”. In case of the vulnerability of rights or data breaches, Article 37 establishes intervention by the data protection officers or delegates. The intervention needs to be activated through complaints delivered to the Data

Protection Authorities. The intervention should accomplish the reestablishment of responsibility data roles. To do that, the officers or delegated might formulate advice, recommendations, and even enforce the organization according to the guidelines of the Data Protection Authorities.

Considering the responsibility to process data, the legislation does not apply to every social domain, yet its implementation is very comprehensive. Data processors that need to abide by these rules are as follows:

a) Professional associations and their general councils.

b) Teaching centers that offer education at any of the levels established in the legislation regulating the right to education, as well as public and private universities.

c) Entities that operate networks and provide electronic communications services following the provisions of their specific legislation, and when they regularly and systematically process large-scale personal data.

d) The service providers of the information society when they develop large-scale profiles of the users of the service.

e) The entities included in article 1 of Law 10/2014, of June 26, on the organization, supervision, and solvency of credit institutions.

f) Financial credit institutions.

g) Insurance and reinsurance entities.

h) Investment services companies, regulated by the market and insurance legislation.

i) Distributors and traders of electricity, energy, and natural gas.

j) The entities are responsible for the evaluation of the solvency and credit, management, and prevention of fraud, including those responsible for the files regulated by the legislation for the prevention of money laundering and terrorism financing.

k) Entities that develop advertising and commercial prospecting activities, including commercial and market research activities, when they carry out treatments based on the preferences of those affected or activities that imply the elaboration of profiles.

l) Health centers legally obliged to maintain the patients' medical records. Health professionals who, although legally obliged to maintain the patient's medical records, exercise their activity on an individual basis are one exception.

m) Entities that have as one of their objects the issuance of commercial reports that may refer to natural persons.

n) Game developers and game activity through electronic, computer, telematic, and interactive channels.

ñ) Private security companies.

o) Sports federations, and sports clubs that process data of minor people. (Article 37.1 of Regulation (EU) 2016/679)

The list above comprises several domains and organizations that should follow personal data protection rules, both in public and market domains. At the same time, the LOPDGDD enhances accountability by enforcement, especially by the sanctions and fine regime imposed over data processors in the scopes above. For example, article 54 allows the DPA to conduct audit plans and monitoring of data processors. The Spanish DPA (Agencia Española de Protección de Datos) may conduct preventive audit plans, addressing the process of data in the above domains. Data processors are obliged to follow the rules of the EU Regulation (2016/679) and the LOPDGDD of 2018. In some cases, the DPA can enforce its sanctioning capacity according to three levels of offenses: Very serious offenses, serious offenses, and minor offenses.

Very serious offenses regard the act of not complying with the law, ignoring the law, or even acting against its fundamental principles (i.e. transferring data to third countries without the consent and guarantees of information security). Serious offenses are enacted when data processors try to comply with the law but they fail to implement it (i.e. to treat data without accreditation, and without performing impact assessments of risks). Finally, minor offenses are dictated when the data processor does not comply with the requirements of the law, but it demonstrates a certain capacity to implement it (i.e. not allowing data subjects to exercise their rights regarding their data).

Important to notice that the LOPDGDD even gives the capacity to DPAs to react in cases of mass surveillance of data subjects under the jurisdiction of the European and Spanish norms. Article 67, based on previous investigation actions, enable the Spanish DPA to investigate facts and circumstances of mass surveillance (like recording or gathering meta-data from huge amounts of personal data without legal guarantees). Yet, the normative is very vague because it infers that "The Spanish Agency for Data Protection will act in any case when the investigation and treatment involving mass flows of personal data is deemed as necessary". The law does not mention specific resolutions or counter-measures aside from subtle sanction capacities enacted by Title IX (articles 70-77 about sanctions and fines). Moreover, the DPA enforcement capacity to address mass surveillance becomes toothless in cases of national security and intelligence interests, and in cases of international jurisdictions that cannot enforce or are

compatible with the DPA recommendations and sanctions. To avoid this scenario, every foreign Data processor handling data from Spanish and European citizens must abide by the GDPR and the LOPDGDD. Yet, the link between different data protection agencies and the capacity to hold accountable international data processors is a case that needs further attention and prospective development. For example, due to the lack of privacy safeguards in third countries, the EU has revoked and updated data transfer agreements with the USA in the last years, such as the 'safe harbor' and 'privacy shield'.[80]

Finally, the LOPDGDD also regulates issues related to basic and general principles of the use of the Internet. Title X regarding Digital Rights (*Derechos Digitales*) aims to preserve the right to the neutrality of the Internet (art. 80) so that internet infrastructures and services treat companies and users in parity of rights (all citizens are equal before the internet, and Internet service operators (ISOs) will provide a transparent service without discrimination based on technical or economic reasons). The same Title ensures the right to universal Internet access (art. 81), the right to privacy and use of digital devices in the workplace (art. 87); the right to digital disconnection in the workplace, the data protection of minors on the Internet, the right to the digital testament, among others.

Recently, in 2020, the Spanish government made a public consult to construct a Chart of Digital Rights. The document is supposed to protect individual autonomy including the right to be untracked or not subjected to personality and behavior analysis that profile people. This Chart also reinforces the right to Internet neutrality. Also, it creates the right to know if automated machines have processed information without human intervention through, and the cases when third party players have sponsored certain information. Also, its ambitious scopes include rights to lead with artificial intelligence. For example, it guarantees the right to no discrimination in decisions based on algorithms. Moreover, it mentions rights in the use of neuronal technologies. In this case, the aim is to preserve individual identity, guaranteeing self-determination and freedom in decision-making, ensuring the confidentiality and security of brain data and thoughts. It is hard to say whether these rights are compatible or can clash against each other or with previous data protection rules. Moreover, it is unclear to express how they can be implemented. At this moment, the Chart does not have a binding effect. Rather, it is a guiding document that aims to define the evolution of digital rights.

[80] *DW News*. 2020, July 16. 'EU court overturns US data transfer agreement in Facebook privacy case', retrieved from https://www.dw.com/en/eu-us-data-transfer-facebook/a-54194377 in 07/23/2020.

5.1.b. Personal data protection in Brazil

In the case of Brazil, the processing of personal data was formally established in 2018 and still awaits to be transposed and implemented. Yet, the topic was addressed partially by previous regulations since the last century, such as the Consumer Protection Code (1990)[81], the Access to Information Law (2011)[82] , and the Internet Civil Framework (2014)[83].

In the late 1990s, Manuel Castells clearly foresaw that the Internet would be the most important global interconnection channel for the decades to come, stating that almost everything would be connected to systems invariably open to people and institutions (Castells, 2004). Hence, legislation in Brazil, as well as in other countries, needed to catch up on the rapid changes produced by digital technologies in the last decades.

As in the case of Spain, the Brazilian legislation is partially inspired in historical international agreements. For example, the International Covenant on Civil and Political Rights of 1966, in Article 17, assures the protection of privacy; as well as the protection of postal mailing, image, intimacy, honor, and reputation of persons. Moreover, article 11 of the American Convention on Human Rights, signed in 1969 in San Jose, Costa Rica, established that "No one shall be subjected to arbitrary or abusive interference in terms of privacy, family, home, correspondence, or against his honor or reputation".

As mentioned in the judicial control of intelligence (Chapter 3), in Brazil privacy is protected by article 5 of the Federal Constitution of 1988, mentioning "privacy, intimacy, honor and image of the people as inviolable rights". In legal terms, private life and intimacy are concepts that generally operate on the same logic, but they should be differentiated to define the scope of their protection. Thus, while privacy and intimacy are related concepts, the difference between them is the particularity that intimacy is any form of communication that excludes a third person whereas privacy is limited to some form of communication that excludes the public or publicity (Avila & Woloszyn, 2017). This is the case, for example, of banking privacy, which involves the communication between one person, the bank, and the Public Treasury Office, while it excludes other actors. Most of the regulations formulated before the Internet were thought in that separation between intimacy and privacy. However, in practice, this differentiation is still debatable nowadays.

---

[81] *Presidência da República*. 1990, September 11. 'Lei N. 8.078'. Retrieved from: http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm in 12/08/2019.

[82] *Presidência da República*. 2011, November 18. 'Lei N. 12.527'. Retrieved from: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm in 12/08/2019.

[83] *Presidência da República*. 2014, April 23. 'Lei N. 12.965'. Retrieved from: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm in 12/08/2019.

For example, in the case of cellphone interceptions (another technology that was universalized or became popular only in the last two decades), the need for regulation, in particular, to add a Chapter in article 5 of the Brazilian Federal Constitution of 1988 was reflected in Law No. 9,296/96. By this, known as the Telephone Interception Law, judicial warrants for the interception of the flow of telephone communications were permitted as a legitimate interference of privacy. Yet, the regulation opts for a criterion of proportionality in the use of the means (wiretapping) that restricts privacy, for serious crimes that imply in the punishment with imprisonment (in the penal sphere), and only when other means are not sufficient to prove authorship or participation in criminal activity. In other words, in the case of privacy and secrecy of telephone communications as a fundamental right, their restriction must be operated in an appropriate, necessary, and proportionate manner (see the principle of proportionality in section 3.6).

With the popularization of the Web, the Brazilian Internet Civil Framework of 2014 aimed to tackle growing problems involving data and communication violations that affected citizens' intimacy and privacy on the Web. This year, the legislators sought solutions to manage and discipline the use of new digital communication technologies, based on the principles of universality, neutrality, and decentralization of the World Wide Web. In Spain, data protection rules were enacted since the 90s but only in 2018 digital rights were regulated more deeply and extensively. In 2018, the LOPDDD adopted those Internet principles as complementary rules for the protection of data. In the reverse sense, the Brazilian scenario did not have a regulation to protect personal data until 2018. Yet, this country enacted the Civil Framework of digital rights in a first moment.

The Brazilian Internet Civil Framework is a sort of Digital Constitution of the country. From the human rights perspective, many goals - especially related to greater social inclusion, freedom of expression, and the fostering of digital culture - can be considered as achievements in the Framework. Yet, the document must be understood as a legal guideline for future Internet legislation. In terms of personal data, Article 10 of the Framework defined the obligation of telecommunication and Internet Service Providers (ISPs) to keep records of metadata and logs, making them available with no judicial order to police and enforcement authorities. Before this norm, Article 17 of Law No. 12,683/2012 allowed police and the Public Prosecution Service to request ISPs files containing information related to metadata (personal logs, affiliation, and address) without the presence of court warrants. Metadata, from the legal point of view, does not belong to the inner circles of personal intimacy. It belongs to the exchanged private information that can be accessed based on a “general” (security, health, economic) interest or to prosecute offenses and crimes. Notwithstanding, from the socio-technical point of view, metadata reveals a lot of information from the intimate life of individuals. The access to metadata can be used to create accurate profiles and characteristics of a person. At the same time, if judicial bodies cannot authorize every interference

of metadata, some mechanisms should be created to connect ISPs with enforcement and state agencies. The access to metadata should not be made through automatic and omnipresent points of connection between ISPs and state agencies, even if they act for the sake of "public interest" or "national security".

Expressions such as "public interest", "social interest", and "national security" constitute vague legal concepts and are frequently claimed to justify restrictions on fundamental rights. In some cases, the loose interpretation of those terms can entail censorship as in China, Iran, Egypt, and North Korea. The wide justification behind those terms serves as a base for blocking websites and as surveillance mechanisms that affect citizens' privacy and intimacy through the monitoring of online networks. As stated by Avila & Woloszyn (2017), those general goals cannot be arbitrarily manipulated by the administration or its agents. On the country, there should be forms to oversee administrative and legal acts that interfere with fundamental rights. Thus, the problem is not the lack of law or acting by illegal channels. The problem is that legal measures used for those purposes should not be a "carte blanche" to automates and unlimited practices that affect privacy and the metadata of citizens.

Most of the time, as in the case of the European Union, data protection come from jurisprudence and higher instances of the Judicial branch. In Brazil, on May 26, 2015, the Supreme Federal Court (STF) authorized the Federal Court of Accounts to access data on loans from a bank (BNDS) that operated public funds in benefit of the meat company JBS/Friboi. This company was accused of corruption, money laundering, and clientelism. Hence, the STF authorized to relativize the right to privacy and intimacy in order to access banking databases. The STF expressed that "the citizenry has the interest to know the destination of public funds". Yet, STF Judges such as Celso de Mello and Marco Aurélio claimed that disclosing banking data would compromise a set of privacy guarantees against abuse and arbitrariness. For them, "if decisions of the Court persist with obvious disregard for the textual provisions of the constitution, serious problems of democratic illegitimacy, illegality and legal certainty would arise".[84] In the end, the data was accessed but no doctrine was formulated to guide the administrative and judicial access to personal data.

After continuous judicial interpretations and the pressure of advocacy groups, Law No. 13,709/ 2018[85] was finally enacted to amend the Civil Internet Framework and provide an overall regulation for the protection of personal data. Acknowledged as General Personal Data Protection Act (LGPD), this measure established personal data and its protection as part of the fundamental rights of

[84] *Supremo Tribunal Federal*. 2015, May 26. 'Operações de crédito entre BNDES e JBS/Friboi não estão cobertas pelo sigilo bancário'. Noticias STF. Retrieved from: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=292332 in 12/10/2019.
[85] *Presidência da República*. 2018, August 14. 'Lei N. 13.709'. Retrieved from: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm in 12/10/2019.

liberty and privacy, which is essential to the free development of natural persons (Article 1). The LGPD is based on informative self-determination rights: freedom of expression, freedom of information, freedom of communication and opinion, the inviolability of intimacy, honor and image, economic and technological development and innovation, free innovativeness, free competition, and consumer protection (Article 2).

The Brazilian LGPD applies to the process of information of a natural person by a legal entity (from public and private law), regardless of the means, the country of the operations, and the place where data is located. The process of information should affect Brazilian citizens or individuals living in Brazilian territory (Article 3). The exception for the LGPD is data treatment for particular/private purposes, or in cases of artistic/academic research, for public safety, national defense, state security, and investigation and prosecution of criminal offenses. In that sense, the Brazilian regulation equals the European RGPD and Spanish LOPDDD in terms of scopes and exceptions.

The LGPD also demands similar standards of data protection for international transfers and considers sensitive personal data as related to "racial or ethnic origin; religious conviction; political opinion; union membership; religious, philosophical or political organization; health or sexual life; genetic or biometric data; and when data is linked with a natural person" (Article 5). Moreover, it mentions three important figures: holder (natural person to whom the personal data subject or the processing refer to), controller (public or private entity who is responsible for decisions regarding the processing of personal data) and operator or processor (public or private entity who processes personal data on behalf of the controller).

The process of data consists of any operation performed with personal data. The operations include the collection, production, reception, classification, use, access, reproduction, transmission, distribution, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, diffusion, or extraction of personal data (article 5). As in the case of the GDPR, the Brazilian LGPD values the explicit and formal consent from the holder to the controller and data processors regarding data quality: accuracy and fidelity, transparency (accessible information about the treatment of data, but preserving trade and industrial secrets), security, prevention, and accountability. In the latter point, accountability is the "proactive demonstration of effective measures in compliance with personal data protection rules" (article 6).

The processing of personal data may only be performed via consent, for the fulfillment of public policies by the administration, for statistics purposes, to protect the life or physical safety, and in commercial and consumer fields (insofar as fundamental rights and freedoms of the holder are respected). Moreover,

anonymous data shall not be considered personal data for this Law, except when the anonymization process can be reversed with feasible technical means (Article 12). Data should be stored, and erased after the end of the treatment period or if requested by the holder; but it can be preserved in research, statistics, and other public documents through anonymization. The LGPD also allows the A.R.C.O. rights (access, rectification, consent, opposition) plus anonymization, deletion of unnecessary data, and portability to another service provider.

The LGPD guarantees commercial and industrial secrets, but it determines that processors and controllers should keep a record of their personal data processing operations, especially when based on legitimate interests (Article 37). In that sense, the national authority may require the controller to draw up a report on the impact of the "protection of personal data, including sensitive data, regarding the data operations, in compliance with this Law and commercial and industrial secrecy regulations" (Article 38). In the same logic entailed by the European legislation, the LGPD demands that the controller shall report to the national authority and to the holder "the occurrence of events that may lead to significant risk or damage to the holders" (Article 48). The reports must include the volume, information, risks, and technical solutions taken to solve the problems.

In that sense, data processors and controllers should follow "good practices" of governance to manage data in different contexts. Those practices are, for example, specific obligations for stakeholders, educational recommendations, internal supervision, risk mitigation mechanisms, and other aspects related to the security of information. When governance fails, the LGPD has also the capacity to enforce administrative sanctions. The minor sanctions consist of warnings acts for the adoption of corrective measures. Major sanctions consist of fines of up to 2% (two percent) of the revenues of the private legal entity, group or conglomerate. The calculation is based on the revenues of the last year, excluding taxes, up to the amount of R$ 50,000,000.00 (fifty million reais) (Article 52).

In addition, the LGPD created the National Data Protection Authority (ANPD), a federal public administration body that is submitted to the Presidency of the Republic (Included by Law No. 13,853/2019). Its financial supervision is regulated through the national budget law. The President of the Republic indicates the Director of the agency after approval of the Federal Senate. The ANPD is autonomous from the technical and decision-making point of view. Yet, the institutional subordination to the Presidency reduces its level of independence if compared to the Spanish AEPD. The ANPD should ensure compliance with commercial and industrial secrets, with the protection of personal data, and the laws that regulate the confidentiality of information (Article 55). Moreover, the ANPD needs to elaborate guidelines for the National Policy of Personal Data Protection and Privacy; and supervise and apply sanctions as established by Article 52. Moreover, the ANPD receives petitions after the processor or controller did not

attend or mitigate holders' complaints. The ANPD has also adjacent missions such as to promote knowledge and awareness of norms and rights of personal data to the population and the cooperation with other agencies from other countries.

Finally, different from the Spanish Case, at least from the formal point of view, the LGPD creates, in article 58, the National Council for the Protection of Personal Data and Privacy. This Council comprises 23 (twenty-three) representatives, holders, and substitutes, from the federal Executive Branch, the two Legislative Houses, from Justice and the General Attorney Office, the Brazilian Internet Steering Committee, representatives of the civil society related to the protection of personal data, scientific/technological and innovation institutions, trade union confederations representing the economic categories of the productive sector, the business sector related to the area of personal data processing, and the labor sector. It aims to institutionalize and create a permanent space for the governance of personal data in Brazil, very similar to the model of the Brazilian Internet Steering Committee that inspired the Internet Civil Framework. The Council proposes strategic guidelines to the National Policy of Personal Data Protection and Privacy and for the ANPD (Law No. 13,853/2019). It is soon to assess activities from the Council as the LGPD awaits to be implemented in the country. In the meantime, the municipal administration of São Paulo tried to sale databases containing information about passengers and cards from the transportation public system. But, it refrained itself after the approval of the data protection law in Brazil.[86] However, the new ANPD and the Council need to increase their strength and cope new challenges. For example, in October, 2020, a leak exposed personal data for millions of Brazilian COVID-19 patients. Months later, the largest personal data leakage in Brazilian history exposed names, unique tax identifiers, facial images, addresses, phone numbers, email, credit score, salary and more from around two hundred million people. Packages containing this information were commercialized in the dark web and on Internet forums.[87] This was only one example of a long series of blatant data leakages, probably only comparable to the Equifax case, when personal data of 145 million people leaked from the US credit bureau in 2016. This example shows the importance of the LGPD and The Council to counteract practices that violate personal data rights. Yet, the law and institutions need to be complemented with the development of a culture of data protection embedded to small and huge organizations across the country.

---

[86] *Privacy International*. 2019, October 17. 'Surveillance and social control: how technology reinforces structural inequality in Latin America'. News & Analysis. Retrieved from: https://privacyinternational.org/news-analysis/3263/surveillance-and-social-control-how-technology-reinforces-structural-inequality in 12/15/2019.

[87] Belli, L. 2021, January 21. 'The largest personal data leakage in Brazilian history', Open Democracy, retrieved from https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+opendemocracy+%28openDemocracy%29 in 02/04/2021.

Epilogue

So far, we have expressed the main aspects of the personal data protection rules by state regulations. Those aspects are summarized in Table 16.

Both in Spain and Brazil, personal data protection rules apply to any organization ruled by public or private law, processing data from natural persons, regardless of the means, the country of operation, and the storage of data. The data must be collected in the territory of those countries. The private and public organizations are comprised of different sectors, from health and education to business, commerce, entertainment, culture, administration, non-profit organizations, political parties, etc. The main data protection rules in both countries are the Spanish LOPDGDD and the Brazilian LGPD. Yet, in the time of writing this, Spain needs to transpose completely the European GDPR and the Brazilian regulation awaits to be enacted and implemented. The exceptions to those rules are information processed for particular/private purposes, in cases of artistic/academic research with anonymous data, for national defense and state security purposes, investigation or prosecution of criminal and administrative offenses, and electronic mass surveillance.

For example, in 2019, anonymized personal data from telecommunication companies was used in Spain to make statistics of transit and demography.[88] In 2020, the same method was applied to watch the confinement and the social distancing of Spaniards during the pandemic crisis caused by the coronavirus. Yet, this raised privacy concerns related to de-anonymization, conservation, and intrusiveness of the gathered data.[89] Also, in October 2020, the Court of Justice of the European Union (CJEU) opened a line in which intelligence, national security, and mass surveillance must be proportional and respect privacy safeguards (such as Directives 95/46/EC on data transfers and 2002/58/EC on privacy and electronic communications). Yet, doubts remain in how State Members will adopt those decisions, whether by creating new judicial mechanisms, new data protection authorities, or if current accountability and institutional bodies would be reformulated. What is clear is that data governance is complex and ever changing.

[88] Maqueda, A. 2019, October 29. 'El INE seguirá la pista de los móviles de toda España durante ocho días'. *El País*. Retrieved from: https://elpais.com/economia/2019/10/28/actualidad/1572295148_688318.html in 12/15/2019.; Romero, O. 2019, October 29. 'El INE quiere rastrear la posición de nuestros móviles pese a que lo impide la ley'. *Público*. Retrieved from: https://www.publico.es/sociedad/privacidad-ine-quiere-rastrear-posicion-moviles-pese-impide-ley.html in 12/16/2019.

[89] Gómez, R. G. 2020, April 1st. 'La UE rastrea los móviles para combatir la epidemia'. *El País*. Retrieved from: https://elpais.com/sociedad/2020-03-31/la-ue-rastrea-los-moviles-para-combatir-la-epidemia.html in 12/15/2019.

Table 16: Accountability and data protection rules.

Accountability dimensions	Cases	
	Spain	Brazil
Who is accountable?	Any organization ruled by public or private law, processing data from natural persons, regardless of the means, the country of operation, and the storage of data, provided the data is collected from/in Spanish and EU jurisdiction.	Any organization ruled by public or private law, processing data from natural persons, regardless of the means, the country of operation, and the storage of data, provided the data is collected from/in Brazilian territory.
To whom are they accountable?	To data protection authorities (European Data Protection Supervisor, Spanish Data Protection Agency, and DPAs in Autonomous Communities). Main regulations: • Charter of Fundamental Rights of the European Union (CFREU) • General Data Protection Regulation of 2016 (European GDPR) (to be transposed) • Spanish Organic Law for Data Protection and Digital Rights or LOPDGDD of 2018 (Replacing Organic Law 254/1993)	To data protection authorities (National Data Protection Authority and the National Council for the Protection of Personal Data and Privacy). Main regulations: • Access to Information Law, 2011 • Internet Civil Framework, 2014 • General Data Protection Act (LGPD), 2018 (to be implemented)
About what are the services accountable?	About legality, purpose, confidentiality, integrity, transparency to process data, and by the definition of specific roles (data subjects, controllers, processors, and data commissioners). Total or partial exception for the LOPDGDD are data treatment for particular/private purposes, in cases of artistic/statistic research, anonymous data, national defense, state security, investigation and prosecution of criminal and administrative offenses, and electronic mass surveillance	About legality, purpose, confidentiality, integrity, transparency to process data, and by the definition of specific roles (data subjects, controllers, processors). Total or partial exception for the LGPD are data treatment for particular/private purposes, in cases of artistic/statistic research, anonymous data, for public safety, national defense, state security, investigation and prosecution of criminal and administrative offenses, and electronic mass surveillance
How are they accountable? (measures)	Organizations should allow subjects to exercise rights over their data: - Access, Rectification, Consent, Opposition, Deletion, Portability. Organizations should follow certain criteria and comply with DPAs mandates by demonstrating - Risk analysis, information security, privacy by design, equivalent data protection rules to transfer data to	Organizations should allow subjects to exercise rights over their data: - Access, Rectification, Consent, Opposition, Deletion, Portability. Organizations should follow certain criteria and comply with DPAs mandates by demonstrating - Risk analysis, information security, privacy by design, equivalent data protection rules to transfer data to

	other countries, conduct reports and audits to external commissioners and DPAs in a proactive manner Organizations might be sanctioned by DPAs through - Preventive and corrective measures Administrative fines from €900 to 600,000, or in case of companies, from €10-20 million or 2 to 4% of the annual turnover revenue budget might be adopted.	other countries, conduct reports and audits when demanded by DPAs Organizations might be sanctioned by DPAs through - Corrective measures Establishing administrative fines up to 2% (two percent) of the revenues of the legal entity of private law, group or conglomerate in Brazil in the last year, excluding taxes, limited in total to R$ 50,000,000.00 (fifty million *reais*).
Assessing accountability according to its internal principles	Did the accountability action result or promote at least one of the following principles? -Answerability -Enforcement (sanctions) -Transparency (passive) ~~-Responsibility~~	Did the accountability action result or promote at least one of the following principles? -Answerability -Enforcement (sanctions) -Transparency (passive) ~~-Responsibility~~

Source: the author

The table also shows that public and private organizations are mainly accountable to Data Protection Authorities (DPAs). In the case of Spain, the DPAs are the European Data Protection Supervisor, the Spanish Data Protection Agency (AEPD), and the Autonomous Communities DPAs. In legal terms, the accounts are especially guided by the Charter of Fundamental Rights of the European Union (CFREU), the jurisprudence from the Court of Justice of the European Union (CJEU), the General Data Protection Regulation (GDPR) of 2016, and the Spanish Organic Law for Data Protection and Digital Rights of 2018 (updating the Organic Law 254/1993 of Personal Data Protection). In the case of Brazil, the organizations will be accountable to the National Data Protection Authority and the Council of Personal Data and Privacy. Until then, the accounts in this country are mainly regulated by the Brazilian Constitution, the Access to Information Law of 2011, the Internet Civil Framework of 2014, and the General Data Protection Act (LGPD) of 2018.

When reporting to DPAs, the array of organizations in both countries will need to demonstrate legality, purpose, confidentiality, integrity, and "accountability" as main principles to process data. "Accountability" in this case is defined as the proactive capacity to deploy measures to comply with the regulations above. Moreover, the organizations need to establish specific roles (data subjects, controllers, processors), defining the persons who are responsible for the treatment of data. In the Spanish case, the transposal of the European GDPR also mentions that external data commissioners (external or independent staff from the organization) should make impact assessment and audits of data protection. According to the main regulations in both cases, organizations should allow data subjects to exercise rights over their data (access, rectification, consent, opposition, deletion, and portability). Moreover, organizations should follow

specific criteria and comply with DPAs mandates demonstrating the capacity to make assess risks, create information security systems, and follow privacy by design principles. They also should consider equivalent data protection rules to transfer data for third countries. To a certain extent, this promotes that data protection rules spread across different countries through the spill-over effect, insofar as many business and commerce practices need to harmonize their standards in a globalized economy. Finally, the organizations subjected to DPAs might be sanctioned through preventive and corrective recommendations. In case of severe faults or neglecting of the recommendations, DPAs in Spain will be able to establish administrative fines from €900 to €600 000 (in case of companies, from €10-20 million or 2-4% of the annual revenue budget). In Brazil, the administrative fines will be up to 2% of the revenues of the legal entity, private group or conglomerate, excluding taxes, and limiting the quantity to R$50 million (fifty million reais).

According to our methodological operationalization, the performance of accountability as a connector between authority and legitimacy is a question of interest. When authority is called to give an account, if that action does not entail more legitimacy, then accountability fails to reach its objective. So far, until the last part of this study, authority was easily attached to intelligence services in a unidirectional relationship where legitimacy increased by the performance of external accountability mechanisms (from internal controls to the media and civil society). In this section, the governance of personal data turns the relationship between authority and legitimacy more complex. Here, we can depict personal data networks in which multiple players can show accountability in many forms. For example, the relationship between data organizations and Data Protection Authorities (DPAs) is not that simple. Most of those organizations (i.e. small and medium-size companies) have less authority when compared to DPAs. On the other hand, certain organizations (especially huge technological corporations from third countries) concentrate bulky data and have enormous authority to regulate the governance of data when compared to other data processors and DPAs. Thus, despite the existence of multiple asymmetries of power between accountable actors, state-regulators still struggle to turn accountable the bulky constellation of data processors.

In light of that, the DPAs can demand answerability and enforcement principles from data organizations. Answerability refers to recommendations and corrections by soft means, that is, through preventive reforms and corrective measures to abide by specific standards (legality, purpose, confidentiality, integrity) and procedures (risk analysis, information security, and privacy by design techniques). Data organizations should follow those measures, otherwise, DPAs can implement accountability by enforcement, by hard corrective measures exemplified in the above regime of administrative fines. However, as explained in this section, despite the devolution of power to implement “good” practices from

DPAs to each organization and company, the recent regulation in both countries is similar and creates new challenges.

For instance, the regulations require comprehensive changes to business practices for companies that had not implemented a comparable level of privacy before (especially in Brazil as the introduction of personal data rules was not regulated until 2018). Since the DPAs cannot oversee the bulky information collected by data processors, it is reasonable to complement institutional roles with a regulation that enhances capillarity to penetrate organizational market functionalities in order to improve accountability –protecting privacy and subject autonomy. The regulations entail a duty of "self-care" or "auto-assessment" beyond legal norms. In that sense, data protection must be a duty for all players dealing with personal data. Nevertheless, we must be skeptical of regulatory mechanisms and "good" practices because they can become fuzzy and elastic enough to be applied to any informational system. For instance, private organizations need to incorporate internal oversight accountability principles (such as horizontal audits and risk assessment) and personal data files must be processed according to the scope and range of each company. In that sense, the new regulation and the new market self-supervision logic could be similar to voluntary compliance in industries impacting the environment. Despite the scheme of fines and enforcement, the efficiency to implement accountability may differ in every company. And, in overall terms, the data environment can still be "polluted". Moreover, certain business models are built around customer surveillance and data manipulation; therefore, voluntary compliance is unlikely (Rubinstein & Good, 2013). It is soon to predict clear results stemmed from the latest regulation of personal data protection. Yet, it is necessary to recognize the potential to improve privacy safeguards, to mitigate the commodification of personal data, and the effort to preserve a certain degree of individual autonomy.

To end this section, two accountability principles still must be considered: transparency and responsibility. In the first principle, the current regulation turns organizations that process data more transparent as they should submit reports and follow DPAs mandates on a regular base. This principle is strongly recommended in the EU and Spain as the GDPR created the role of data commissioner, an external and independent figure that must have access to the information systems and audits of each organization to verify the accomplishment of data protection rules. In the case of Brazil, there is no mention of this role in the LGPD and doubts remain if the recent regulatory framework will be efficiently implemented across the country. Even old regimes such as the European one had problems of institutionalization and coordination between many DPAs. Despite the recent creation of those roles in 2018, one problem of this notion of transparency is that organizations still tend to remain in a passive role. They should deliver reports and give credentials to commissioners, in doing so, they can adapt reactive policies to show transparency and abide by rules. Rather, they would need to

internalize this principle in every aspect of their systems and databases, as expressed by the proactive recommendations. Moreover, the regulations turn organizations transparent until a certain point insofar as industrial and commercial secrets remain inaccessible to inspections and external controls. Those blind spots can be used as shields to turn core functions such as algorithms and information cycles immune to data protection rules. Finally, transparency can be fostered in the side of the citizen (the watched), and neglected or ignored in the side of strong data processors from the state/market (the watchers). In that sense, the mentioned metaphor of "slides of visibility" (Bakir & McStay, 2015) is very useful to scrutinize transparency schemes in the governance of personal data.

When it comes to the principle of responsibility, the ability to fulfill missions and duties, many obstacles can emerge despite the good intentions of the regulatory framework. Responsibility increases insofar as organizations abide by DPAs mandates and standards. Responsibility also increases as users have access to exercise their rights to customize or delete their data, and when DPAs enforce and demand more transparency to protect sensitive information of people. These actions encourage standards to avoid discrimination, manipulation, disinformation, commodification, and intrusive interference of data. However, responsibility has especially been transferred to the users and to a heterogeneous array of organizations that can dilute any data protection effort.

For users or data subjects, responsibility has been managed through self-management of privacy (Solove, 2013). That is, from the user perspective, consent has become an irreflexive and automatic act, especially in those cases in which its granting operates as an unavoidable condition to access a certain benefit. Thus, it is important to develop other sources of legality such as integrity, transparency, and accountability, as postulated by new data protection norms.

For data processors, as the balance of risks and benefits are different in each organization and social domain, respecting the legal standards of data turns the governance in this realm very heterogeneous. The scheme of responsibility in this domain is fuzzy and fluid as technological developments modify the collection, process, use, and interpretation of data, turning the control of organizations even harder when compared to traditional regulatory arenas such as labor inspection and environmental policies. The legal regime of data protection cannot regulate the bulky information collected by data processors in a full sense. Thus, responsibility is passed to companies that have particular strategies to manage privacy and information related to subjects' autonomy. Responsibility, in ultimate sense, depends on self-supervision and voluntary compliance. Now we turn to assess market strategies in the governance of personal data.

5.2. Market strategies

In this section, we address the market strategies to process data. First, we examine the Internet as an economic domain that has changed the understanding and the way business players operate data. In sequence, we examine the forms to turn accountable giant technological corporations that operate at the global level. We end this section showing complementary mechanisms related to accountability, such as accountable algorithms, privacy by design principles, and the growth of oligopolies in the data business.

5.2.a. Internet and data business

At the beginning of this century, few people around the globe knew or had accounts related to nowadays common companies such as Google, Facebook, Amazon, Apple, Netflix, Spotify, etc. In the current state of things, most of the Spanish and Brazilian citizens work and live using those platforms. The next decades probably will see the emergence of new platforms, and, in the long future, maybe the disappearance of some. Yet, in the last two decades, it became increasingly normal to find digital platforms that operate within the logic of the "algorithmic culture", monitoring, analyzing and filtering a huge volume of data (big data) to offer personalized browsing experience to their users. As in the case of the Radio, TV, and other mass media communication forms in the early twentieth century, the management of information by digital organizations based on algorithms to process data is marked by the presence of few conglomerates and giant brands that configure the culture and the production of cultural goods. For example, in 2017, Google and Apple controlled 99% of the market related to smartphone applications in the world, aside from China.[90]

The rise of the algorithmic culture is similar to previous communication industries and technologies in the sense that the high cost of technology for the production of goods, the mastery of a complex distribution network and the growing need for investments in advertising are all factors that presuppose the existence of large initial capital. In economic theory, large capital is required to produce income or return to scale (in which the return on profit only comes after massive investments), something that small or medium-sized business organizations traditionally cannot afford. Such a reality tends to undermine the chances of many companies to participate in different business sectors and makes

[90] Vincent, J. 2017, February 16th. '99.6 percent of new smartphones run Android or iOS'. *The Verge*. Retrieved from: https://www.theverge.com/2017/2/16/14634656/android-ios-market-share-blackberry-2016 in 12/20/2019.

concentration on oligopoly arrangements of companies in real competition a common configuration (Bezerra, 2017).

Located in the USA territory, the major music and film industries of this country have "oligopolized" throughout the twentieth century the international market for the production, distribution, and marketing of mass cultural goods. Since the 1990s, the popularization of the use of sound, visual and written digital techniques, and the consolidation of the Internet have opened new spaces and channels to agents in the information mediation regime. However, some decades after the rise of the Internet, as in the case of the cultural industry during the last century, it became common to find few tech companies dominating more than three-quarters of their respective markets. In addition, it must be added something that economists call "network effects," in which users or costumers tend to follow the leader companies in one sector, creating the so-called "herd behavior" (Sun, 2013). Therefore, instead of several companies competing in free conditions, now we see as "normal" the concentration of about 90% of a market sector by one company, such as Google (created in 1998) in the sector of the online search engine, or Facebook (created in 2004) in the sector of digital social network (Haucap & Heimeshoff, 2014) (Moore & Tambini, 2018).

Holding networks of billions of users, these companies take advantage of the opportunity to use huge amounts of personal data for business purposes, earning most of their profits from personalized advertising distribution. On the Internet, users do the semiotic work in the frontend while algorithms and engineers develop the backend production of informational "goods" to users. In the case of the giant platforms above, algorithms seek to predict what kind of information will be of interest to each individual and, at the same time, to use this information to give personalized experiences (which includes advertising but not only) back to users (Striphas, 2015). In other words, this resembles the constant production and consumption of users' data in a retro-alimentation circuit of information between user-platforms-user to produce add-value "experiences". Meanwhile, the circuit monetizes those informational experiences to third players and to the "owners" of the platforms. It means the total fusion between production and the means of production (from/in users), in a perfect circuit that keeps capitals, information, and goods being distributed into few shareholders and owners of the backend door. As explained in the first part, this circuit is conducted at the expense of the monetization of individuals' information and their consequent alienation (Fuchs, 2011). We will retake the issue of the data market in the last part of this Chapter.

Those are some of the material conditions sustaining the digital market of big data processors today. In addition, the material infrastructure of the internet is a field of disputes between market players as in the case of transmitting and selling content to Internet users. At this point, one essential point is the so-called net

neutrality to transfer data. Ramos (2014) identifies network neutrality as the prohibition imposed over network operators to block or slow users' access to certain content or applications. This relates to the prohibition of charging differentiated tariffs for access to certain content or applications and the obligation to maintain transparent and reasonable traffic management practices. In other words, if we think data flows as pipelines, the owner and companies that provide services through the pipelines are supposed to let flow the content regardless of the origin and users' demand.

To its supporters, network neutrality seeks to preserve the foundations that have made the Internet an instrument for innovation, participation and cooperation, and user empowerment (Belli & Foditsch, 2016). The absence of this principle would allow Internet Service Providers (ISPs) to customize or censor content available on the Internet. In this perspective, the extraordinary diversity of information circulating on the global network would be negatively impacted by the end of the neutrality principle (Schafer, Musiani, & Le Crosnier, 2014). However, other people support new uses to the Internet architecture, affirming that data flows must be differentiated allowing distinct Quality Standards of Service (QoS) (Hahn & Wallsten, 2006). This would make data more reliable and delivered according to "pay-for-play" demands and priorities. In this logic, ISPs may filter access to applications, content, and services; according to demand and consumers' preferences (Brennan, 2010). A sort of filtering includes zero-rating, which is characterized as a price customization modality in which certain companies provide free data traffic associated with specific content or applications. Furthermore, in the restricted data vision, some data needs to travel faster or free, as in the case of emergency communications, and to expand and deliver data networks for the poorest and remote areas.

In Brazil, pay-for-play content is sponsored by certain companies during commercial campaigns, such as Netshoes Group e-commerce site, Privalia Online Store, Natura cosmetics, Mercado Livre e-commerce (a kind of Brazilian Amazon), Bradesco Bank Free Access, and Santander Bank free access apps (Silva, Bergmann, & Marques, 2019). However, those are few cases compared to the universe of companies and entities that operate on the Web. Moreover, net neutrality is considered as one of the milestones of the Civil Internet Framework in Brazil. Law No. 12,965/2014 was enacted after a drafting process that lasted seven years involving companies and civil society. The Framework enshrined three essential pillars: freedom of expression, user privacy, and network neutrality. In that sense, data processors should treat data packets without distinction by content, origin, service, terminal, or application. According to the legislation, the creation of private subdomains on the World Wide Web by telecommunications infrastructure owners would undermine the original architecture of the Internet, which established an open network based on the free circulation of information and knowledge (Belli & Foditsch, 2016). In that sense, Brazil has taken an important

role in this battle by designing a model of Internet governance based on multi-stakeholder participation, enshrining a regulation that supports net neutrality in this country (Leite & Lemos, 2014).

In the case of Europe, civil society and data processors discussed these issues from 2013 to 2016. In those years, the General Data Protection Rules (GDPR) of the EU reinforced the principle of net neutrality. In February 2018, the German coalition between the governing parties CDU/CSU and SPD agreed that the so-called "upload filters" were not appropriate to use the Internet. Those filters were also rejected during the civil society campaign “save the internet”.[91] In Spain, the mentioned LOPDDD ensures the principle of net neutrality in order to allow further digital rights and general access to information regardless of the data and demand for content. Notwithstanding, at the international level, a backslash effect emerged when the Federal Communications Commission (FCC) of the USA derogated net neutrality in this country in 2017. By Donald Trump’s appointment of Ajit Pai, the FCC reversed previous net neutrality rules. The FCC's decision was contested by states and companies supporting net neutrality. Corporations such as Amazon, Spotify, and Netflix expressed their desire to restore net neutrality in 2018. The same year, the campaign was also supported by Facebook and Google.[92] As several states and ISPs challenged this modification, the Federal Circuit Court of Appeals ruled in October 2019 that the FCC can reclassify this issue. Yet, the Court also expressed that the FCC cannot block state or local-level net neutrality. Hence, as in the case of other enforcement and sensitive policies in the USA, net neutrality has a mixed regulation within the levels of the federation.

5.2.b. Accountability of big market players

In this part, we address the accountability forms of big corporations such as Facebook and Google. This is explained because they can be considered as hegemonic actors or powerful market players who process bulky amounts of data at the global level (including Spain and Brazil). Facebook and Google are the main market players regarding social networks and search engine browsing. In addition, those players are good examples to show the relationship between data processors and data subjects in our cases.

In the case of Facebook, after its creation in 2004, the corporation has expanded over the world, being considered as one of the backbones of data

[91] *Koalitionsvertrag zwischen CDU, CSU und SPD*. 2018, March 12. ‘Ein neuer Aufbruch für Europa’. Berlin. From: https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1, consulted in 12/17/2019.

[92] Thadani, T. 2018, January 5. ‘Facebook, Google, Netflix join fight to restore net neutrality’. *San Francisco Chronicle*. Retrieved from: https://www.sfchronicle.com/business/article/Facebook-Google-Netflix-join-fight-to-restore-12477404.php in 12/19/2019.

globalization. As this proceeds, several dilemmas have arisen in terms of responsibility and transparency to process and protect data. In 2018, Facebook was in its biggest public relations crisis ever. The alleged distortion of information (disinformation), the spread of unreal and controversial information (misinformation), and the Cambridge Analytics scandal, in which a third company elaborated profiles and data records of users without their consent for political and scientific purposes, challenged Facebook image and market position. As a result, the corporation was held accountable even by the United States Congress in an open session that was broadcasted worldwide.[93] The outcomes of this legislative accountability action put Facebook against the ropes in terms of prestige and trust from governments and users. To answer this, the company started changing its notoriously opaque policies and products to better reflect a newfound commitment with transparency and trust.[94] For example, Facebook announced an update, allowing users to verify ads that the website is currently running. Before this case, there were very few ways in which page owners could be held accountable for the ads they ran. A page could "dark post" hyper-targeted ads into users' news feed (such as Instagram) and there would be no clear way to tie the ad back to the organization that paid for it. After that change, Facebook expressed that "Transparency has become something of a catchphrase for the company over the last years as it scrambles to restore trust following a spate of high profile scandals. With each update, Facebook has sworn that transparency is top of mind."[95]

As typical in scandal situations, Facebook desperately needed to win back users' confidence by hyping its commitment to transparency and users' demands. A company as large and influential as Facebook should be as transparent as possible. But it's difficult to ignore that most of the time provisional solutions or patches can be applied after scandals. For instance, ProPublica, a marketing company that uses a plugin to verify which kind of ads a user receives on Facebook, protested against the Facebook update because it disabled its plugin in the social network. ProPublica plugin worked thanks to the fact that if the user told Facebook she/he is "liberal", this person might see ads for liberal causes. But, according to the agency, this sort of targeting can also get much more granular, and this explains why Cambridge Analytica targeted people with political ads based on their preferences, influencing the United States presidential campaign in 2017. Similarly, tools such as Mozilla "WhoTargetsMe" were also disabled due to the

[93] Kleinman, Z. 2018, March 21. 'Cambridge Analytica: The story so far'. BBC News, retrieved from www.bbc.com/news/technology-43465968 in 12/18/2019.
[94] Bell, K. 2018, June 29. 'Facebook is pushing 'transparency' hard, but it's becoming a crutch'. Mashable, Tech. Retrieved from https://mashable.com/article/facebook-transparency-ad-strategy/?europe=true in 12/17/2019.
[95] Idem

changes made on Facebook's policies.[96] Facebook alleged that the actions were made to prevent widgets and plugins from scraping the personal information of users for privacy and security reasons. However, both ProPublica and Mozilla were skeptical of those allegations. Richard Tofel, ProPublica president, expressed "They [Facebook] claim this is because of potential abuse or because of problems with such tools, but they have cited no evidence. No such problems have resulted in our Political Ad Collector, and Facebook knows it."[97] Marshall Erwin, Mozilla's head of trust and security, expressed that "Major tech companies need to provide more transparency into political advertising, and support researchers and other organizations, like Mozilla, working in good faith to strengthen our democratic processes."[98] Facebook maintains its own searchable database of political advertising, but this tool was only available in three countries (the USA, UK, and Brazil). Even in those countries, the Facebook reports do not explain the use of information that is associated with advertising plugins and third companies.

Targeting has been a major source of controversy for Facebook since Cambridge Analytica whistleblower Christopher Wylie revealed that his company's ads were able to "psychographically profile" users. The efficiency of micro-targeting is still under debate in fields such as psychology, political marketing, and business fields.[99] However, the ability to reach a highly customized group of potential customers is central to Facebook. This company is valued as an ad platform and more scrutiny could threaten its current business model based on plugin companies and advertising partners. Transparency advocate groups have also criticized this change: "This appears to be a deliberate attempt to obstruct journalism focused on Facebook's platform […]. We cannot trust Facebook to be its

[96] Kraus, R. 2019, January 30. 'Despite 'transparency' claims, Facebook stops watchdogs from monitoring ads'. *Mashable, Tech*. Retrieved from https://mashable.com/article/facebook-ads-transparency-propublica/?europe=true&utm_source=internal&utm_medium=onsite in 12/17/2019.

[97] Idem

[98] Idem

[99] Political science professor Travis Ridout, the author of "The Campaign Power of Political Advertising said "What evidence do we have out there that microtargetting is highly persuasive? There isn't much" […] "We can know which magazines you subscribe to, and which type of car you drive, and all of that information, and you can do the fancy stats on that. And it really isn't going to gain you much more than knowing if the person is registered as a republican or a democrat." But there's also evidence that using psychographic profiles to microtarget political messaging could be a sea change for candidates and issues. Rob Smith, a professor of marketing at the Ohio State University Fisher School of Business, and co-author of a study on how microtargeted advertising affects people's behavior and sense of self, views tactics like those employed by Cambridge Analytica and the Trump campaign as highly successful in motivating real-world action: "If a political party can focus their marketing budget on undecided voters, or specifically to an undecided voter that may be leaning a certain direction but not planning to vote, that is clearly a lucrative segment to target." In Kraus, R. 2018, March 24. How well does 'microtargeted psychographic advertising' work anyway? *Mashable, Tech*. Retrieved from https://mashable.com/2018/03/24/how-microtargeted-ads-affect-behavior/?europe=true in 12/18/2019.

own gatekeeper"[100]. In that sense, the updates of Facebook policies to prevent the exposure of people's information to third organizations might mask a lack of commitment to deeper transparency procedures in this corporation. And if only the companies certified by Facebook can access the data, then the company is filtering the transparency of its internal procedures in advance. Thus, major forms of accountability need to be explored. Companies like Facebook and other social networks, given their size and importance in economy and politics, should lift restrictions impeding transparency and clear research on those platforms

Therefore, what other kinds of accountable actions have been given by giant data processors like Facebook or Google? In both cases, it is possible to formulate four layers or categories do demand accountability from big tech corporations in a general sense that applies to many countries, including our cases.

1. **Public frontend layer** (the public part of contents and news showed to users in websites), in which data processors can be obliged to monitor or even delete information. No administrative or judicial authorization is needed to intercept data as the information is available to the public.
2. **Private frontend layer** (the restricted visible/shared part of contents and news showed to specific users in websites), in which data processors can be obliged to monitor or even eliminate information. Administrative or judicial authorization is needed to alter data.
3. **Backend layer** (the "hidden" part related to the processing and technical management of data in servers and material infrastructures), at the **metadata level** (less sensitive information of users). Here, administrative (no judicial) authorization is enough to intercept data.
4. **Backend layer** (the "hidden" part related to the processing and technical management of data in servers and material infrastructures), at the **core data level** (core and sensitive information of users). Here, judicial authorization is needed to intercept data

The first layer can be understood as traditional public spaces such as markets, streets, squares, and even the interior of certain private spaces that are public like malls, restaurants, shops, etc. In this layer, enforcement and private companies can monitor and gather information on the Web with no considerable restrictions, as in the case of car patrols surveilling streets. For public purposes, Facebook can be considered a sort of private mall or virtual infrastructure where users enter to communicate using different tools as the company sells their information. If a Facebook post has a "public" audience, the information can be accessed with no legal restrictions by external players. This virtual space is subjected to norms and

[100] Abdo, A. 2018, September 15. 'Facebook is shaping public discourse. We need to understand how'. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2018/sep/15/facebook-twitter-social-media-public-discourse in 12/18/2019.

rules as physical spaces. In that sense, the information in this layer can even serve to collect proofs by enforcement agencies in investigations and criminal prosecution. The cyberspace is far from being the free space or absolute reign of everything goes. This kind of monitoring can be found even in the deep web (not-indexed websites) and in the dark web (not-indexed websites and illegal niches), where police agencies can monitor public forums and public websites as car patrols monitor "unnamed streets" or "dark alleys" in suburbs of big cities.

The second layer is similar to the previous one, but the difference is that the content is not public but private. For example, it refers to posts and information shared between members and restricted audiences. Thus, enforcement authorities and external monitoring players need legal authorization to access or eliminate users' information published by data processors like Facebook. The legal authorization, expressed in the form of judicial warrants, allows the monitoring and deletion of content as in the case of hate speech, anti-terrorism, and copyrights issues. In these cases, police agencies request judicial officials to contact platforms like Facebook or Tweeter to disable private content in the frontend, the informational part of contents and news seen by users on websites.

The third and fourth layers are related to sensitive issues in the backend, the information architecture that is not visible for normal users on the websites. It refers to the technical aspects (security of information systems, informational policies, and administrative roles) and material infrastructures (cables, terminals, servers) to process data. In these layers, the companies manage the roles and policies of their websites, as well as filter and enable content in the frontend. This is the backstage of platforms like Facebook. Here, the management is regulated by the rules of data protection (see the previous section), enforcement law, market law, and technical and business practices from informational players themselves.

In the third layer, data processors such as Facebook, Google, and Internet Service Providers (ISPs) are obligated to store records of metadata (logs, IP addresses, user names, and basic account information) and deliver it to enforcement and legal authorities if requested. The requests can be done without judicial warrants. Metadata is supposed to be less sensitive or to be in the outer circles of privacy, thus, its availability does not require judicial counteractions to be accessed. However, administrative authorization is needed as meta-data itself can reveal patterns that allow monitor and surveille profiles in a deeper manner especially when correlated (matched) to information gathered in other layers. In this layer, mass surveillance of meta-data with no legal checks and proportionality means were perpetrated by agencies such as the NSA as documented in the Snowden Revelations in 2013. Since then, many ISPs started to encrypt their platforms and services to protect data and to maintain trust and confidence from users.

In the fourth layer, processors like Facebook or Google protect their data and keep the "keys" to access core data from users as this sensitive information relates to inner circles of privacy. Core data refers to the content of messages, video-calls, emails, and private posts stored by data processors. This kind of data is supposed to be protected during its transmission or record in this backend layer. As access to this data entails the suspension of many fundamental rights, in this layer, enforcement and legal authorities need to present judicial warrants to ISPs.

The access to metadata and core data is easier when ISPs are coopted or collude with enforcement authorities and governments, as in the case of regimes that deploy points of access to request the keys of encryption or copies of data in a direct and regular base (i.e. the Great Firewall in China). The collusion between those players –state and data giants- is more difficult when authorities cannot hold accountable ISPs and data processors. In this situation, enforcement authorities depend on the jurisdiction of the companies (usually located in third countries) and on the predisposition of data processors to cooperate with them.[101] Thus, the asymmetry of power between public authorities and market players entails different results for the cooperation and the transfer of data. Yet, that kind of coordination, and surveillance in an overall sense, can be established by legal channels, as in the case of the layers above. When legally implemented, the same points that allow intrusive and disproportional monitoring of populations can be converted to reach legitimate purposes and to demand more transparency and accountability of market players.

One can even mention a fifth layer, where surveillance and monitoring are unregulated and exercised beyond visible tools of control and codes of the market. A field in which there is no trust, monitoring is ubiquitous, and no rules apply to access information and data. This field indeed exists but escapes from every legal notion and reasonable principle. As examples, one can mention the case of illegal use or commercialization of wiretapping tools by corrupted officials in Spain and Brazil,[102] and mass surveillance programs such as the NSA Prism revealed by Edward Snowden that violated the domestic and international law. This layer is the most difficult to be regulated and usually escapes from the range of accountability. Yet, the fifth layer can be counteracted by the improvement of the judicial control to authorize access to data and by assessing the quality of legal mechanisms that authorize the interference of fundamental rights. In that sense, the judicial

[101] Uruguay, for example, is a country that has admitted problems to conduct investigations and track criminal groups. Its surveillance programs like "Guardian" are incapable of monitoring WhatsApp conversations. See *Subrayado*. 2017, June 05. "Jueces y fiscales admiten que software espía no sirve para rastrear WhatsApp". Retrieved from https://www.subrayado.com.uy/jueces-y-fiscales-admiten-que-software-espia-no-sirve-rastrear-whatsapp-n67508 in 12/20/2019.
[102] In Spain, operation *Tandem* and *Cloacas de Interior* case, Prosecutor's Office and even some judges and police chiefs colluded to construct parallel networks to the service of clientelistic relations with businessman and politicians (Fort, 2017). In the case of Brazil, the market for illegal eavesdropping among police officers, and the role of militias, is a challenge due to its extension and parallel forms to conduct investigations beyond the control of justice (Carpentieri, 2016).

oversight should avoid automatic points of access and cannot be converted in a legal mask to facilitate transfers of data (see Chapter 3, section 3.6). This layer can also be counteracted by extending international cooperation and improving transnational networks of accountability (see Chapter 3, section 3.7).

Considering the above layers, in the first layer, information is available to the public in the frontend (the visible part of contents and news showed to users on a website). In the second layer, in general, an administrative or judicial authorization is needed to alter data. For example, public authorities can present administrative petitions or judicial warrants to edit or delete private publications in the frontend. Here, the problem is that enforcement actions might collide frontally with freedom of speech and civil liberties, such as during the Spider Operation (*Operación Araña*) that ruled a series of antiterrorism sentences that targeted artistic and intellectual expression in Spain.[103] In the third layer, no judicial authorization is needed to intercept metadata. However, administrative petitions or requests based on proportionality principles might be presented to the companies.

In Spain, for example, police or enforcement agencies can present administrative petitions from the Minister of Interior leader to access logs, IPs, geolocation, etc. Nonetheless, because of this unchecked authority, former Interior Minister Fernández Díaz became suspect for conducting the National Police without judicial warrants to protect his party and monitor political adversaries until 2016.[104] This issue arises the dilemma of police autonomy and their legal control by judicial courts, a critical point also observed in Brazil when the president Bolsonaro intervened in the Federal Police autonomy to dismiss director Mauricio Valeixo in order to shield his family in corruption investigations.[105] The President itself would have used parallel intelligence structures to defend his relatives against prosecutors and justice courts.[106]

Finally, in the fourth layer, public authorities can only present judicial warrants to the companies in order to access core data stored in the backend (part related to the processing and technical management of data in servers and material infrastructures). Here the problem is to assess the quality of the authorizations as many courts can be overwhelmed by petitions or can formulate the warrants in an

[103] Torrús, A. 2017, November 21. 'La cara B de las acusaciones de los fiscales por enaltecimiento en redes sociales'. *Público*. Operación Araña. Retrieved from https://www.publico.es/sociedad/operacion-arana-cara-b-acusaciones-fiscales-enaltecimiento-redes-sociales.html in 04/13/2020

[104] Romero, J. M. 2018, December 16. 'El exministro Fernández Díaz usó hasta 2016 a la policía para ayudar a su partido'. *El País*. Retrieved from https://elpais.com/politica/2018/12/15/actualidad/1544903992_074446.html in 04/27/2020

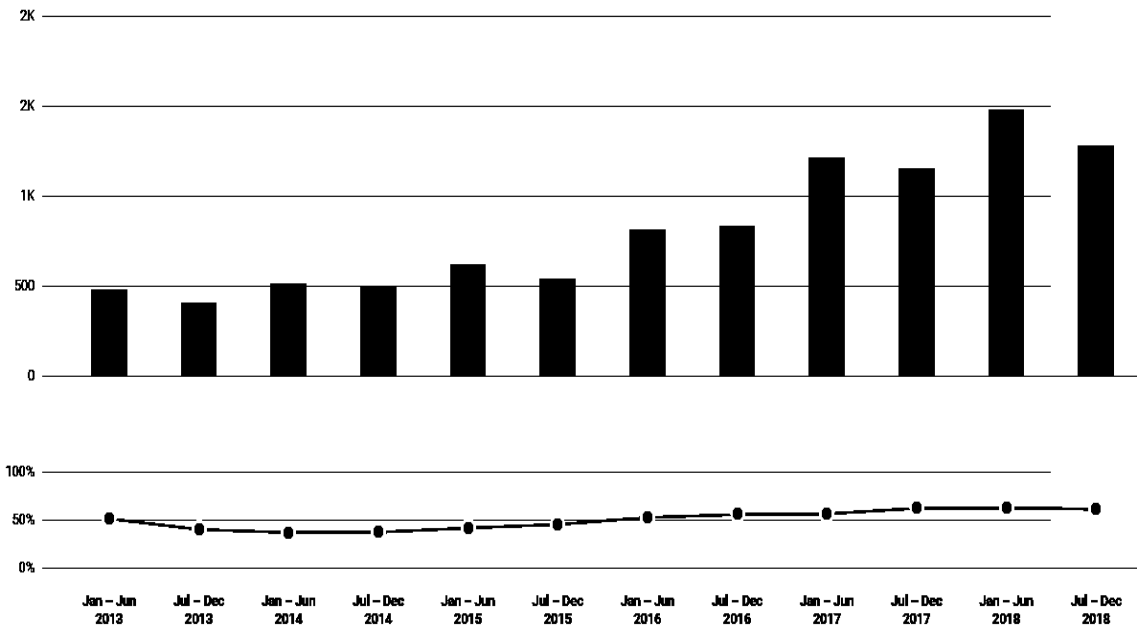
[105] *BBC Brasil*. 2020, April 24. 'Bolsonaro nega que tenha interferido na PF'. News. Retrieved from https://www.bbc.com/portuguese/brasil-52420754 in 04/30/2020

[106] Últimas Noticias, 2020 December 11. 'They ask to investigate if Brazilian intelligence helped Bolsonaro's son', retrieved from https://en.ultimasnoticias.com.ve/news/general/They-ask-to-investigate-if-Brazilian-intelligence-helped-Bolsonaro%27s-son/ in 12/14/2020

"automatic" base, without deeper evaluations of the investigations and data interventions. This might be the case of Spanish courts as they have a debatable capacity to supervise the use of the Integrated System of Legal Interception of Telecommunications (SITEL) by security agencies and the police.[107]

In recent times, companies like Facebook have created reports to show transparency and to clarify how corporations react when they disclose personal data from their users. In our cases, Spanish and Brazilian authorities (both administrative and judicial) had requested to access data from this company. Figure 14 below shows the volume of requests and the percentage of approvals or disclosed petition by Facebook each year (from 2013 to 2018).

Figure 14: Facebook transparency reports in Spain



Source: the author (based on facebook.com)

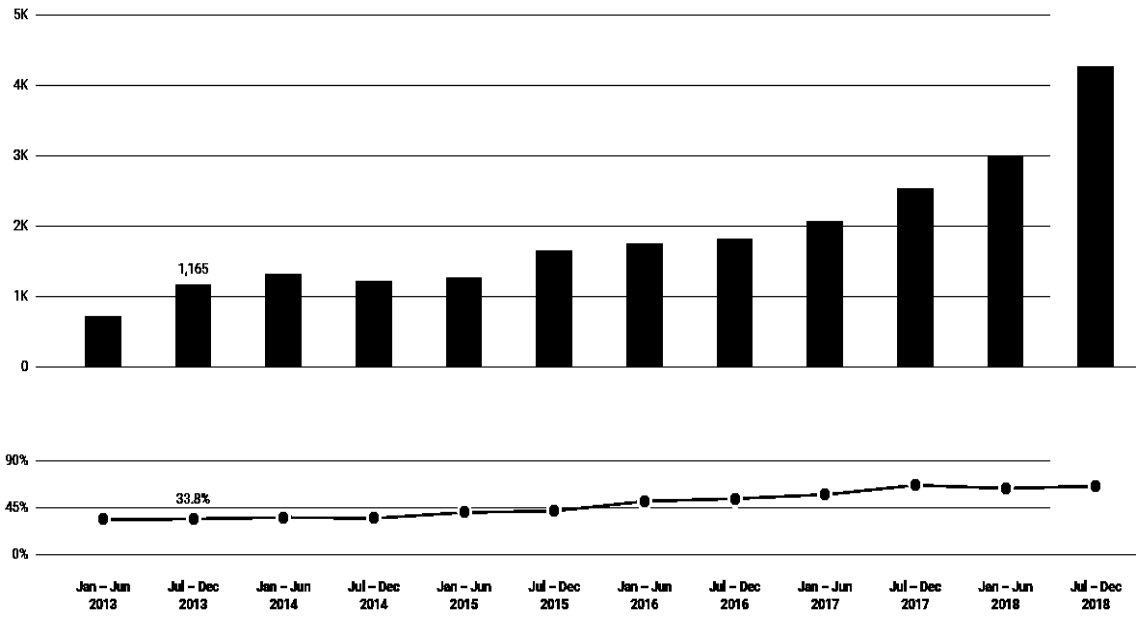
In the case of Spain, between January and June of 2013, there were 479 requests. 51% were disclosed or produced data to authorities and external controllers. In the last semester of 2018, Facebook received 1,277 requests, and

[107] The alleged lack of efficiency and oversight of the courts regarding SITEL interceptions can be exemplified by Tuset, G. B. 2013, October 28. 'NSA y SITEL, dos caras de la misma moneda'. El Diario, Zona Crítica. Retrieved from https://www.eldiario.es/zonacritica/NSA-SITEL-caras-misma-moneda_6_190790927.html in 12/20/2019. The SITEL continues to advance slowly at the risk of becoming obsolete by technological changes, such as the expansion of mobile phone applications (González Hernández, 2018). However, SITEL financial budget has increased in the last decade, and one of their programs, SILC, created in 2008, has been improved to intercept encrypted communications from social networks such as WhatsApp, Telegram, and Signal. See López-Fonseca, O., 2020, July 17. 'Interior gasta 15 millones al año en su sistema de espionaje de comunicaciones'. *El País*. Retrieved from https://elpais.com/espana/2020-07-16/interior-gasta-15-millones-al-ano-en-su-sistema-de-espionaje-de-comunicaciones.html in 07/17/2020.

61% produced data. According to the reports, Facebook responds to government requests for data following applicable law and its terms of service. “Each and every request is carefully reviewed for legal sufficiency and we [Facebook] may reject or require greater specificity on requests that appear overly broad or vague”.

In the case of Brazil (see Figure 15), between January and June of 2013, there were 715 requests. Only 33% were disclosed or produced data to authorities and external controllers. In the last semester of 2018, Facebook received 4270 requests, and 65% produced data. Both countries presented growing petitions in absolute terms in the historical series. Brazil has almost a double amount of petitions than Spain, but the percentage of requests that produced data are similar in both countries (around 60%). Besides, only in recent years (since 2016), Facebook has approved more than 50% of the petitions as some of these contained errors, were legally vague or inconsistent with Facebook policies.

Figure 15: Facebook transparency reports in Brazil



Source: the author (based on facebook.com)

In Brazil, the cooperation between data controllers and Facebook has been improved especially after 2016. In March 2016, a critical situation happened when the Federal Police (PF) arrested Diego Dzodan, Facebook Vice President for Latin America. According to the PF, Facebook violated court orders to transfer information. The information required from the company was supposed to support “the production of evidence in secret police investigations against organized crime and drug trafficking”.[108] According to the PF, the company refused the petition and

[108] Borges, R. 2016, March 1st. ‘Diego Dzodan, vice-presidente do Facebook para América Latina, é preso pela Polícia Federal’. *El País Brasil*. Retrieved from

was fined R$ 50,000. Enforcement authorities raised the fine to R$ 1.000.000 (one million reais) and Dzodan was prosecuted. In December 2015, a similar episode occurred when the Facebook application for messages Whatsapp was shut down during 13 hours in the whole country by the judicial order of the First Criminal Court of São Bernardo do Campo in São Paulo. Due to the secrecy of the criminal investigation, enforcement authorities never confirmed the real motivation of the order. However, at that time, the media mentioned the motif was related to the reluctance of the tech company to deliver core data for an investigation involving drug trafficking. WhatsApp responded affirming that the company does not store users' messages and was "extending a strong end-to-end encryption system", which means users' messages are totally protected.[109] According to WhatsApp, no one, nor criminals, the police, or even the company itself can intercept or read the messages. However, it is known that strong organization can deploy technical aspects to dodge encryption and obtain meta-data and core data from mobile applications. Every digital interaction, even when protected by encryption, leaves prints that can be traced especially in the weakest steps of the information cycle, i.e. when users send or read data. In short, encryption might be 100% safe, but there is no 100 % safety when apps or software are processed in electronic devices and hardware. Reading a message in a smartphone or sending an email in a computer requires an environment comprised of default hardware settings, information cycles, frontend and backend definitions, and user behavior; elements that are impossible to be tamed in their totality for the sake of security.[110] Yet, intrusive methods to dodge encryption and access data are illegal if used without judicial warrants by police or security agencies. For example, in 2009 the Inter-American Court found Brazil guilty of improper telephone interception of agricultural workers and activists for not complying with legal standards. The interceptions were conducted in the "fifth" layer: by inappropriate authorities, out of an ongoing investigation, and without notification to the Attorney General's

https://brasil.elpais.com/brasil/2016/03/01/tecnologia/1456843819_998702.html in 12/20/2019.

[109] Sreeharsha, V. 2016, May 2nd. 'WhatsApp Blocked in Brazil as Judge Seeks Data'. *The New York Times*, technology. Retrieved from https://www.nytimes.com/2016/05/03/technology/judge-seeking-data-shuts-down-whatsapp-in-brazil.html in 12/22/2019.

[110] When cryptographic data is sent through a network, at a certain node or stage of its life cycle, it needs to be processed by a computer. Even if the information is scrambled and its integrity along the flow is assured, the moment the user access the file to visualize it, after applying his/her decrypt key, it needs to be processed by internal algorithms in the processer. Hence, the data will be processed while decrypted. And since current technologies are yet to be able to process encrypted data, during this task, guaranteeing confidentiality becomes almost impossible. There is nothing to impede unauthorized access and collection of communications' content during this point of its cycle. NSA programs like QUANTUM, which is able to inject malicious software in almost any computer connected even to those not connected to the Internet, could easily develop backdoors and malwares to have access to information during the very moment of processing (Monteiro, 2014). In Spain, one of the SITEL programs, SILC, created in 2008, has been improved to intercept encrypted communications from social networks such as WhatsApp, Telegram, and Signal. See López-Fonseca, O. 2020, July 17. 'Interior gasta 15 millones al año en su sistema de espionaje de comunicaciones'. *El País*. Retrieved from https://elpais.com/espana/2020-07-16/interior-gasta-15-millones-al-ano-en-su-sistema-de-espionaje-de-comunicaciones.html in 07/17/2020.

Office.[111] In other case, the Brazilian Federal Police contracted controversial malware from the 'Hacking Team Company' to target and monitor communications in the context of the Olympic Games as mentioned in Chapter 3, section 3.8.

In light of the above, one can mention that Facebook was accountable for enforcement principles. That is, sanctions and even judicial actions were imposed on the company when it refused to transfer data to public authorities through legal petitions. Yet, when it comes to examining the quality of accountability, few conclusions can be extracted from that cooperation. For example, the official requests of data are circumscribed to collect proofs for ulterior judicial prosecution or as part of criminal investigations. Thus, Facebook is not being assessed by the forms to process personal data, but by the capacity to disclose and transfer data to authorities. In that sense, Facebook might collaborate with public authorities by default, labeling this cooperation as transparency. Indeed, the reports suggest that Spanish and Brazilian administrations have demanded more data from foreign giant market processor during the last years. But the requests need to be contrasted with the number of users in each country (about 80 million in Brazil and 20 million in Spain in 2018).[112] Furthermore, the requests should be understood as final actions taken by administrations when conducted in criminal law and enforcement procedures. That is, the number of requests is supposed to be the last resource used by public authorities to clarify serious offenses. In this case, after other methods fail, the urgency to request data from Facebook would avoid a proper evaluation of the internal policies and data activities conducted within the company. For example, the Spanish LOPDDD and the Brazilian LGPD regulations do not address judicial requests of data processors such as Facebook. Moreover, in the cases personal data protection laws apply to companies such as Facebook (for example, in international data transfers, in the rights of data subjects over their personal information, and in terms of the general management and process of data), the laws still preserve the commercial and business secrecy from companies. At the end of the day, Facebook algorithms prevail to categorize and profile users, matching and selling filtered information to third processors and companies, and offering a more "personalized experience" to users.

In the case of Google, another giant data processer, there are also transparency reports about the second and fourth layers of accountability. That is, public authorities had also requested access to specific accounts, users, and

[111] In 2013, 21,925 telephones and 1563 e-mails were legally intercepted by enforcement authorities in Brazil. See Becker, S.; Lara, J. C.; Canales, M. P. 2018. 'La construcción de Estándares legales para la vigilancia en América Latina'. Parte I: Algunos ejemplos de regulación actual en América Latina. *Derechos Digitales*, documentos. Retrieved from: https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-I.pdf in 12/22/2019.

[112] *Statista*, 'Number of Facebook users in Brazil from 2017 to 2023'. Retrieved from https://www.statista.com/statistics/244936/number-of-facebook-users-in-brazil/, Data for Spain in https://www.statista.com/statistics/283633/spain-number-of-facebook-users/, accessed in 01/11/2020.

information from this company. Google expressed that "We publish this information [the reports of transparency] to publicize the impact of government actions on our users and the free circulation of information online." The company has prepared those reports since July 2010 to reflect the number of requests it has responded to external actors. According to the technological company,

> When we receive a request for information about users, we review it carefully, and only provide information within the scope and authority of the request. The privacy and security of the data that users entrust to Google are fundamental to us. Before providing data in response to a government agency's request, we ensure that it complies with Google's law and policies. We notify users of these legal requests whenever appropriate, unless prohibited by law or court order. And if we believe that a request is not accurate, we try to limit it, as we did by convincing a court to drastically limit a request from a US government agency whereby data corresponding to two months of search queries from a user were requested.[113]

It is relevant to notice that Google releases a transparency report including the Foreign Intelligence Surveillance Act (FISA). FISA was promulgated in 1978 to regulate how the American Government gathers foreign intelligence for national security purposes. Based on this law, the Foreign Intelligence Surveillance Court (FISC) is comprised of 11 federal judges that review requests by government agencies for electronic surveillance and other types of intelligence data collection. The Foreign Intelligence Court of Appeal was also created to ensure defense and appeals to FISC resolutions. These courts can require companies and other private organizations to disclose information for foreign intelligence investigations.

Under the FISA, USA government agencies may request court orders from the FISA Court to, among other actions, require US companies to provide personal information of users and the content of their communications. Since 2008, those requirements include core data of the communications associated with the accounts of non-US citizens or illegal permanent residents outside the United States. The Department of Justice supervises the agencies involved in carrying out the activities authorized by FISA. This law requires these agencies to inform the Congress regularly and submit all relevant documents of the FISA court. In that sense, even Google is submitted to government agencies' requests. And, as in the case of Facebook, "before providing information to respond to such a request, we [the company] ensure that it adheres to Google's law and policies. If we believe that one of those requests is too broad, we try to limit it."[114] Users and non-US citizens are not informed when companies receive requests based on those acts,

[113] *Google*. 'Transparency Report'. Retrieved from https://transparencyreport.google.com/?hl=en in 01/13/2020.
[114] *Google*. 'Transparency Report. United States national security requests'. Retrieved from https://transparencyreport.google.com/user-data/us-national-security?hl=en in 01/13/2020.

especially when US security agencies consider that the publication of those requests would "endanger the national security of the United States or the life or physical security of other persons, interfere in diplomatic relations, criminal investigations, counter-terrorism, and intelligence operations."[115] In the case of FISA applications, current legislation prohibits recipients of such requests from revealing their existence.

Table 17: Google transparency report. USA national security requests per year

Periodo de informe	Número de solicitudes	Usuarios/cuentas
jul. 2018-dic. 2018	Los datos están sujetos a un retraso en el periodo de informe de 6 meses	Los datos están sujetos a un retraso en el periodo de informe de 6 meses
ene. 2018-jun. 2018	500 – 999	97000 – 97499
jul. 2017-dic. 2017	500 – 999	65000 – 65499
ene. 2017-jun. 2017	500 – 999	48500 – 48999
jul. 2016-dic. 2016	500 – 999	35000 – 35499
ene. 2016-jun. 2016	500 – 999	25000 – 25499
jul. 2015-dic. 2015	500 – 999	22500 – 22999
ene. 2015-jun. 2015	500 – 999	19000 – 19499
jul. 2014-dic. 2014	500 – 999	18500 – 18999
ene. 2014-jun. 2014	500 – 999	17000 – 17499
jul. 2013-dic. 2013	500 – 999	15500 – 15999
ene. 2013-jun. 2013	500 – 999	14000 – 14499
jul. 2012-dic. 2012	500 – 999	12500 – 12999
ene. 2012-jun. 2012	500 – 999	10500 – 10999
jul. 2011-dic. 2011	500 – 999	10000 – 10499
ene. 2011-jun. 2011	500 – 999	7000 – 7499
jul. 2010-dic. 2010	0 – 499	4000 – 4499
ene. 2010-jun. 2010	0 – 499	3500 – 3999

Source: google.com

In the third and fourth layer of accountability, Google receives Metadata Requests by the US agencies, such as the IP addresses associated with a particular account or the fields referring to the sender ("from") and the recipient ("to") of the email headers in Gmail accounts. In the fourth layer, Google receives Content Requests from a user's account, such as Gmail messages, documents, photos, and

[115] Idem

YouTube videos. Table 17 shows those Requests under the US National Security Legislation. From left to right the variables are "period of request", "number of petitions", and "user/accounts". According to Google reports, the number of petitions has oscillated between 500 and 999 in each period regardless of the year. However, the variable "users/accounts" related to those petitions has increased from 3500-3999 in 2010 and 18500-1899 in 2014, to 97000-97499 in 2018. As in the case of Facebook, the numbers here are an image of the role of US agencies and their increasing role alongside ISPs and data processors worldwide.

However, the number of requests from the Table should be read carefully since the amount depicts petitions from all the foreign countries where Google operates. Yet, it serves as a clue to show the exponential growth of the Internet and Google users (as well as the expansion of smartphones and apps) around the world during the last years. Is virtually impossible to know how many of those petitions relate to Spanish or Brazilian users and accounts. However, the document gives an example of how market players can contribute to some basic level of accountability. From the perspective of national security and foreign intelligence, Google Reports are one example of "deferred" transparency. The Reports contribute to the access of information, especially in a field of sensitive petitions, without compromising the national security and safety of countries. Yet, the same critiques applied to Facebook reports can also be transferred to Google.

To some extent, giant data processors have awakened to transparency in order to show some level of accountability, especially when they have faced requests from governments after the war on terror since 2001 and as a consequence of the universalization of digital networks around the world. In the case of Google, since 2006, before publishing the first Transparency Report in the history of the Web, the company has faced many government requests to obtain information from users and, sometimes, it has stood out as one of the few companies that refused to accept these requests. Although the reluctance was the exception to the norm, the relations between market players and government agencies have been market by collisions in important cases related to privacy.[116] In 2010, Google requested authorization from the Homeland Security Department to release the Transparency Reports. In April 2012, Twitter began to disclose information about the effect of government requests to freedom of information on the Internet. In the following year, Microsoft, Apple, and Facebook followed and made the generation of transparency reports a recurring practice throughout the data industry. In 2013, security and online surveillance have become important issues, such as Edward Snowden's disclosures, Sony hacking, the dilemmas of encryption, and so on. In this year, Edward Snowden's disclosures revealed that

[116] Beyond Google reluctance, see the responses of Apple to unencrypting IPhone security protocols in the light of crime investigations by the FBI. See *Digital Trends*. 2016, April 3. 'Apple vs. the FBI: A complete timeline of the war over tech encryption'. Retrieved from https://www.digitaltrends.com/mobile/apple-encryption-court-order-news/ in 01/15/2020.

the NSA requested information from Verizon Company about phone calls on a continuous and daily basis. In June 2013, Google responded to claims about the NSA program PRISM on mass surveillance when Larry Page and David Drummond, general manager and general counsel of the company respectively, denied any participation to give the US government (or any other government) direct access to servers.[117] However, they mentioned that the PRISM event confirmed the need for a more clear approach and highlighted the importance of transparency teports. Besides, in March 2014, Google started using connections with HTTPS encryption for querying and sending emails. HTTPS is secure and coded keys to protect data transfers between senders and receivers on the Web. This change, adopted also in the same period by other technological companies, means that no one can see the messages as they flow between users. This makes harder the monitoring of Content Data (but not impossible) and legally speaking creates a scenario in which security agencies and administrations, in general, must present judicial authorization to request this kind of data to ISPs or other data companies. This can explain, in part, the rising number of petitions as verified in the tables above.

Finally, to turn corporations such as Google more accountable, we need to remind that they have several stakeholders and partners from a different scale. For example, in its classical and main market activity, Google sells profiled information to enhance analytics and advertisement. If a person has a website, a blog, or any other kind of presence on the Internet, Google has a way to monetize it. Programs such as Google AdSense serve to put advertisements in the correct place and moment, making ads relevant to the specific content of a web page. For instance, if someone navigates in a website that covers the latest golf tournament, Google could serve ads for golf clubs or golfing attire. The owner of the website can get paid every time someone clicks on one of those ads. This is called Cost Per Click (CPC) advertising. With the right combination of traffic, content, and users, if somebody has a blog or website that gets 100,000 visitors every month, or more than 1 million every year, it could mean a click-through rate (CTR) of 1%, which is standard (Hu, Shin, & Tang, 2010). In that example, 1% of 100,000 is 1,000. If the CPC of the ad is $0.01, the website owner receives $10. If the CPC of the ad is $1.00, the amount rises to $1,000, and so on. Those values can be insignificant if considered in terms of large companies and revenues obtained in other services. Yet, in the world of small companies and start-ups, this system has created a market arena where an array of players dispute information from search engines and social networks, promoting a competition to create the "most attractive" content, in order to maximize incomes.

Therefore, there is no use to turn accountable giant corporations if accountability does not address market strategies even in small and medium-sized

[117] *Google*. 'Transparency Report. United States national security requests'. Retrieved from https://transparencyreport.google.com/user-data/us-national-security?hl=en in 01/13/2020.

companies. That is, not only accountability must gain capillarity to penetrate in different scales of business, but it also should penetrate the core functionalities and strategies of market players. In that sense, the last section of this chapter examines further approaches of accountability in crucial aspects such as algorithms, privacy by design, and the role of oligopolies of data.

5.2.c. Further approaches: algorithms, privacy by design, and oligopolies

Accountability of algorithms is crucial because data processors and dataveillance relate to this activity, from the formulation and implementation of information systems to decision-making in private and public organizations. Thus, computer science and engineering professionals have a role to play here. While autonomous decision-making is the essence of algorithmic power, the human influence in algorithms are many: criteria choices, optimization functions, training data, and the semantics of categories, to name just a few. In a market economy where "prioritizing is something we do on a daily basis to cope with the information onslaught" (Diakopoulos, 2015, p. 3), algorithms prioritize information in a way that emphasizes certain things at the expense of others. By definition, prioritization is about discrimination. As a result, there may be consequences to individuals or other entities that should be considered during design. "Search engines are canonical examples, but there are many other consequential rankings —from the quality of schools and hospitals to the riskiness of illegal immigrants on watch lists" (idem, p. 14).

In that sense, algorithms made for classification might affect people's opportunities because of bias, uncertainty, and outright mistakes in automated classification. The training data that is the basis for supervised machine-learning algorithms is an important consideration, given the human biases that may be lurking there. Also, Sen et al (2015) underscore the need to consider the cultural community from which training data is collected. In developing classification algorithms, hence, designers must also consider the accuracy of the classifications: the false positives and false negatives association. "Decisions revolve around creating relationships between entities. The semantics of those relationships can vary from the generic "related to" or "similar to" to distinct domain-specific meanings. These associations lead to connotations in their human interpretation (Diakopoulos, 2015). The criteria that dictate how closely two entities match are engineering choices that can have implications for the accuracy of an association, both objectively and in terms of how that association is interpreted by other people.

> "One issue with the church of big data is its overriding faith in correlation as king. Correlations certainly do create statistical associations between data dimensions. But despite the popular adage, "Correlation does not equal causation," […] This all indicates a challenge in communicating associations and the need to distinguish correlative vs. causal associations […]. Nowadays, even filtering content and censorship in digital platforms is made by algorithms. Online comments are sometimes filtered algorithmically to determine whether or not they are anti-social and therefore unworthy of public consumption. Of course, the danger here is in going too far—into censorship. Censorship decisions that may be false positives should be carefully considered, especially in cultures where freedom of speech is deeply ingrained (Diakopoulos, 2015, p. 5).

Those issues demand to question the better forms to develop and turn accountable algorithms. Here, there is no single answer as those equations are mutable and used in an array of contexts. There are side effects that developers should notice beyond the engineering aspects of the algorithms, such as the human contexts, responses and the way automated decisions cope with sensitive data treatment such as race, ethnicity, religion, nationality, gender, sexuality, disability, marital status, or age in inappropriate ways. In that sense, ethics needs to be incorporated throughout the engineering process, reconsidering the consequences of the unlikely false positive and the way criteria are measured and defined in training data sets.

In the case of the public sector, citizens elect a government that provides social goods and exercises its power in a way that is moderated through norms and regulations. The government is legitimate only to the extent that it is accountable to the citizenry. But algorithms are largely unregulated now, and they are indeed exercising power over individuals or policies in a way that in some cases (e.g., hidden government watch lists) lacks any accountability whatsoever. "We, the governed, should find it unacceptable that there is no transparency or even systematic benchmarking and evaluation of these forecasts, given the important policy decisions they [the algorithms] feed" (Diakopoulos, 2015, p. 8).

Corporations, on the other hand, do not have the same mandate for public accountability, though they may sometimes be impelled to act through social pressure (e.g., boycotts, responsibility, trust, satisfaction, sustainability, etc). Perhaps more compelling is the capitalist argument that higher data quality and thus better matches and inferences will lead to more satisfied customers. However, given the impact of algorithms in governance and in collecting and refining data from users, the clearest way to correct their impact is to design processes that adjudicate and facilitate the correction of false positives by end-users. Beyond external pressures, companies should allow public audits and users to inspect, dispute, and correct inaccurate labels in the data, improving overall data quality

for machine-learning applications. The data protection rules address databases and security of information, recommending transparent algorithms, but there is too much room to regulate the accountability of algorithms through internal and external oversight. As in the case of national security and intelligence, sensitive algorithms from companies that are protected by industrial secrecy can be more transparent without compromising their functions and efficiency. Indeed, many private algorithms depend on public forums and open codes to be build and implemented (Wieringa, 2020).

Again, transparency can be a mechanism that facilitates accountability, one that we should demand from the government and exhort from the industry. Corporations often limit their transparency out of fear of losing a competitive advantage from a trade secret or of exposing their systems to gaming and manipulation. Complete source-code transparency of algorithms, however, is overkill in many if not most cases. Instead, the disclosure of certain key pieces of information, including aggregate results and benchmarks, would be far more effective in communicating algorithmic performance to the public. "When automobile manufacturers disclose crash-test results, they don't tell you the details of how they engineered the vehicle. When restaurant inspection scores are published by local municipalities, they don't disclose a restaurant's unique recipes" (Diakopoulos, 2015, p. 9). The point is that there are models for transparency that can effectively audit and disclose information of interest to the public without conflicting with intellectual property and trade secrets.

In addition, audit trails could help accountability by recording stepwise correlations and inferences made during the algorithm prediction process. Benchmark guidelines should be developed when a government uses an algorithm, triggering an audit trail. This would allow interested parties, including journalists or policy experts, to run assessments of the government algorithm, benchmark errors, and look for cases of discrimination or censorship. "For example, someone could take two rows of data that varied on just one piece of sensitive information like race and examine the outcome to determine if unjustified discrimination occurred".[118] In some cases, a more adversarial approach may be necessary for investigating black-box algorithms. In the domain of journalism, Dörr & Hollnbuchner (2017) affirm that algorithmic accountability is crucial to calibrate ethical balance from the institutionalization of automated procedures in this field such as quantum computing, natural language processing, neuronal networks, and non-supervised artificial intelligence.

[118] "One avenue for transparency here is to communicate the quality of the data, including its accuracy, completeness, and uncertainty, as well as its temporality (since validity may change over time), representativeness of a sample for a specific population, and assumptions or other limitations. Other dimensions of data processing can also be made transparent: how was it defined, collected, transformed, vetted, and edited (either automatically or by human hands)? How are various data labels gathered, and do they reflect a more objective or subjective process?" (Diakopoulos, 2015, p. 12).

Accountability here involves sampling algorithms along key dimensions to examine the input-output relationship and investigate and characterize an algorithm's influence, mistakes, or biases. Moreover, it involves the transformation of language (objectivity, authorship, transparency) to identify and discuss professional codes (deontological procedures) at the intersection of digital media ethics and cyber ethics. As an example, algorithmic journalism can reshape the traditional investigative accountability journalism, which for many years has had the goal of exposing malfeasance and misuse of power in government, corporations, and other social institutions. In this and other examples, regarding the use of platforms and data systems, Annany & Crawford (2018, p. 985) argue that "making one part of an algorithmic system visible—such as the algorithm, or even the underlying data—is not the same as holding the assemblage accountable". They argue that is necessary to go beyond micro technical transparency to hold organizations accountable, assuming its limitations and potentials to look at socio-technical aspects (i.e. power relations, culture, professionalization, key actors, etc.) that cut across any organization. In Spain, scholars such as Carles Ramió have also expressed that the public administration needs a proactive role to verify and assess algorithms in a digital governance that includes citizen participation, co-management of services, collaborative systems, and public-private partnerships (Ramió, 2019).

Furthermore, the challenging aspect to turn algorithms accountable is to create bonds with ethics and policy systems. Automated procedures, and not only algorithms, redefine the sense of politics and public interest, as well as the role of business organizations. This requires continuous legal updates in this field, as the mentioned Chart of Digital Rights in Spain (see section 5.1). Yet, at the end of the day, even with the rise of techniques such as neurological technologies, better artificial intelligence, and new forms of computing, ethical and human aspects must be there. Technical systems are fluid, hence, any attempt to disclose them has to consider the dynamism of machines that might always learn from new data. Thus, the technical and engineering culture needs to become ingrained with the idea of continuous human feedback. Human-computer interaction must always be connected, at least in different scales and procedures such as assessment and supervision. Besides, focusing only on technical aspects could enhance a fluid technocracy in which computer engineers and first-hand informatics professionals can become the first victims of their "success".

At the same time, data processors from the market have been concerned about the best forms to integrate technical and human aspects to manage sensitive information by exploring functional and technical solutions. Beyond algorithms, "Privacy by Design" (PbD) claims that IT systems must take privacy into account from input to output processes. For example, privacy is a variable to be considered from software design to electronic delivery of services. Devices and applications such as WiFi routers, social networks, and search engines must provide privacy

tools (access controls, encryption, provisions for anonymous use, etc.) embedded in the core functions of those products.

A comprehensive definition of PbD was coined by Cavoukian (2009) by seven principles. These principles could be related to accountability in IT systems as they promote: 1. Proactive and preventive measures to counterbalance privacy risks, 2. Privacy protection as default in any IT system or business practice, 3. Privacy embedded in the core functionality of the system delivered, 4. Positive-Sum, not Zero-Sum approach, to avoid false dichotomies, such as privacy vs. security, 5. End-to-End secure lifecycle management of information, 6. Visibility and Transparency, operating data according to the stated promises and objectives, and subjecting IT systems to independent verification, and 7. User-Centric Designs to keep the interests of the individual uppermost by offering strong privacy defaults, appropriate risk alerts, and empowering user-friendly options.

In short, PbD tries to conceal privacy management across IT Systems, accountable business practices, physical design, and networked infrastructure. Despite its comprehensiveness, some people have claimed that PbD ideas to mitigate privacy concerns and achieve data protection compliance remain vague and leave many open questions about their application in engineering systems (Gürses, Troncoso, & Diaz, 2011). For Scharr (2010), PbD could be difficult to be translated into practice. For instance, data collectors can articulate the purpose specification to include any data of their liking, eliminating the need to consider data minimization (especially in countries where data protection rules are flaw). Furthermore, companies can limit the reach of solutions that they provide by applying anonymization over aggregated personal data, which means that they can process personal data outside of the range of data protection rules insofar as the anonymous data is not reverted or identified to specific persons. The efficiency of data in terms of accuracy and commercial value can shrink when anonymization is applied. Yet, the definition of privacy by design is therefore also "susceptible to the interpretation to collect any data as long as it is with a privacy label while shrinking the scope of control from the user" (Schaar, 2010, p. 270).

Despite those concerns, market players recognize that privacy must be protected as a vital component of nowadays e-commerce and business. To avoid an image of dire lucrative corporations that exploit personal data as a simple commodity, some companies started to adopt "good" practices to process data. One example is the ISO.IEC 27000 series of standards on Security Management published by the International Organization for Standardization and the International Electrotechnical Commission. Those standards dominate how information security management is done today in cloud services and telecoms. When an organization obtains a 27001 certification, it means that a third party has verified that the organization implements information security standards and follows appropriate technical requirements. In turn, these requirements must be

updated frequently to reflect the new developments of technology and to respond to the risks against personal information in each company.

Those and other third parties certifications could be deemed as accountability horizontal strategies that include trustworthiness and reputation among IT suppliers (important symbols that serve as political coins in this domain). For instance, a survey from Orange upon its customers mentioned that "fully 78% of consumers think it is hard to trust companies when it comes to using their personal data" (The Future of Digital Trust Convention, in Kearney, 2014). Other companies are immersed in a rhetoric effort to mitigate privacy risks by opposing the fear and uncertainty that privacy is always traded off against public safety and security. The European Union Agency for Network and Information Security (ENISA) working on information security expertise for the EU and its Member States, and The International Chamber of Commerce (ICC), in addition, have defined some similar accountability principles for business organizations in international forums (Figures 16 and 17).

Figure 16: Linking near-term solutions to market core challenges

	Transparency	Accountability	Empowerment
Standard data taxonomies	• Drives transparency by creating a common language. • Enables meaningful transparency by filtering what is relevant from what is not. • Facilitates interoperable identity and trust frameworks.	• Provide a baseline for interoperable permissions.	• At the coarse-grained, after level, I can translate technical details into personally relevant themes. • Empowers individuals with context-aware data usage and interoperable data use policies.
Measuring risks and benefits	• Assist data controllers and regulators to set priorities. • Promote global interoperability and leverage existing risk management methodologies.	• Creates a workable measure by which to hold organizations accountable.	• Restructures risk around the concerns and needs of individuals. • Provides institutions with the ability to understand perceived harms through the eyes of individuals.

Source: World Economic Forum (Kearney, 2014)

Figure 17: Linking long-term solutions to market core challenges

	Transparency	Accountability	Empowerment
Context-aware personal data management	• Demonstrate that the flow and usage of data (and metadata) is consistent with agreed upon norms and legal requirements. • Meaningful user agreements. With better data accounting, risks can be redistributed.	• Provide the technical means to uphold shared principles in a dynamic, recursive and complex ecosystem. • Strengthen confidence on restitution across jurisdictions.	• Enable individuals to express their unique preferences and controls via metadata. • Individuals can dynamically manage data within a defined context.
Accountable algorithms	• Focus on communicating the intended impact to individuals. • Transparency into the underlying values, principles, decision criteria and outcomes of algorithms.	• Cross-disciplinary "algorithmists" who are collectively responsible for auditing the ethics and anticipated social impact of data driven outcomes.	• Strengthened popular understanding on the economic, sociological and ethical value of the sovereign individual who is both a data producer and consumer.

Source: World Economic Forum (Kearney, 2014)

As observed in the last two figures, the ICC accountability principles are closely related to Privacy by Design principles as they cover different sectors such as engineering, business management, and friendly-user environments. In this view, transparency enhances accountability that in turn improves empowerment through near-term and long-term solutions. Those solutions are related to standard taxonomies, risk measurement, context-aware personal data management, and accountable algorithms. Adopting those solutions in the perspective of data processors implies that a company "demonstrates that the flow and usage of data (and metadata) is consistent with agreed-upon norms and legal requirements" (Figure 16). In addition, "strengthen confidence" and "empower individuals" over their personal data are at the core of systems and functionalities. In that sense, risk analysis assessment is to be encouraged as well as the assessment of auditable algorithms. For example, the latter should "anticipate the ethical and social impact of data usage" (Figure 17).

At first glance, those solutions could be deemed trivial ones. In fact, they have introduced a new paradigm for business practices that cannot be neglected to analyze the participation of market players in contemporary forms of politics. The figures show that the accountability principles of market players –such as telecommunication companies and IT processors- now are much related to the accountability supported by state legislators. This convergence is verified in the "General Data Protection Regulation" (GPDR) attested in the same principles (audits, accountable algorithms, risk and impact assessment, fluid and proactive accountability, etc) incorporated by data-protection laws (LOPDD and LGPD) in Spain and Brazil.

In short, gathering personal information entails a duty of care and protection beyond legal regulations. Data protection must be a duty for all players dealing with personal data. Nevertheless, we must be skeptical of market principles such as Privacy by Design and other "good" practices because they can become fuzzy and elastic enough to be applied to any informational system. "Given such a fate, […] privacy by design would risk being damaging to all involved: if the principles are applied loosely, it would lead to a false sense of privacy and trust, until the term loses its reputation enough to become meaningless" (Schaar, 2010, p. 271).

The market principles and the state regulation indicated are positive insofar as they expand the range and the social dimensions for the accountability of personal data. Theoretically saying, those changes offer the chance to consider privacy more seriously and increase the data subjects' autonomy over their data. By allowing data rights and improving accountability processes adopted by each data processor, the current politics to sort and administer populations can be mitigated in favor of subjects. However, if accountability aims to reduce the asymmetry of power between data processors and data subjects, then this must

move beyond the best market principles and data protection rules. In other words, the role of the civic agency must also be considered as a sphere that can fulfill accountability demands in the face of market and state accountability limitations. We will return to this point in the next section.

We close this section as we started it, mentioning that the digital market is not detached from material constraints and infrastructures. For this reason, the recent battles over data and the clashes between administrations and companies have moved into the discussion about the monopolies of giant tech companies. In 2017, the German regulation body that monitors market competition has ordered Facebook to stop some of its core activities, unless it gets more explicit user consent. Those activities include combining the Facebook gains about users from external websites into their backend Facebook profiles, as well as combining the accounts of people on Facebook-owned companies, including WhatsApp and Instagram.[119] To defend its market position, Facebook alleged actions both in privacy and competitive grounds. Facebook mentioned that the market regulatory agency shouldn't have jurisdiction over the protection of data as "the GDPR specifically empowers data protection regulators – not competition authorities – to determine whether companies are following up to their responsibilities."[120]

Nevertheless, the regulation of digital market monopolies has become important because companies such as Apple, Alphabet (the multinational conglomerate restructured in 2015 and headed by Google), Microsoft, Amazon, and Facebook have accumulated so much power that they have an excessive influence on various parts of the economy (see Figure 18 below). The mentioned tech corporations are the largest entities by market capacity. It means they are the most valued companies by investors in absolute terms. The list would be slightly different if we consider the ranking of revenues, profits, assets, and market value.[121] In that case, Chinese state and private companies are taking the leader position in the top list in terms of inversion and revenues. Yet, in terms of valorization and market capacity, the figure serves as a picture of the evolution of the structural economy in recent decades, a moment in which commodity and energy companies have been replaced by tech companies. And this trend would be foreseen at least in the next decades because the digital market is more flexible and unique to produce added-value products and services. For example, traditional logistic companies like Walmart need to build more stores, expand complex supply

[119] Kraus, R. 2019, February, 07th. 'Germany orders Facebook to stop combining user data from multiple sources into one'. *Mashable, Tech*. Retrieved from https://mashable.com/article/germany-orders-facebook-stop-combining-user-data/?europe=true&utm_source=internal&utm_medium=onsite in 01/20/2020.

[120] Idem

[121] *Global Finance*. 2019, August 29. 'World's Largest Companies 2019'. Retrieved from https://www.gfmag.com/global-data/economic-data/largest-companies in 01/21/2020.; *Forbes*. 2020, April 24. 'The World's Largest Public Companies. The List'. Retrieved from https://www.forbes.com/global2000/list/ in 01/21/2020.

chains, and hire new employees. This takes a lot of capital and manpower, and the stakes are high for each new expansion. Amazon, on the other hand, can bring in more revenues with less of the work or risk involved. The scale allows tech companies to get bigger without getting dragged down by traditional logistics and economic variables. This explains why the expansion of digital apps steers the development of cooperative platforms in other levels of the economy, such as in micro and medium-sized business. In these levels, those platforms have proliferated even in traditional domains such as tourism and private transportation, enabling the conditions to dodge or make flexible labor stakes and economic costs in a process called "Uberization" of the economy (Daidj, 2019). In that context, big tech companies are also able to gain competitive advantages that are extremely difficult to supplant. While oil companies are fighting over a limited supply and have a commoditized end product, Google and Facebook have key businesses that are truly unique and turn personal data –and persons by extension- into retro alimentation commodities that allow a constant supply to deliver services.[122] After the rise of the dot.com bubble, the expansion of telecoms and mobile companies, today we live in an era in which business data companies, especially from the USA and China, dominate the market at the global level.

Figure 18: The largest companies in the world by market capacity.

Source: visualcapitalist.com

[122] Desjardins, J. 2019, March 29. 'How the Tech Giants Make Their Billions.' *Visual Capitalist*. Retrieved from https://www.visualcapitalist.com/how-tech-giants-make-billions/ in 01/21/2020.

Considering the structural economic position of the giant tech companies, Khan (2016), in "Amazon's Antitrust Paradox", contradicts the consensus that has existed in antitrust circles since the 1970s: If the consumer is happy because prices are competitive and services are good, the market works. For her, tech giants have too much data from consumers and obtain many advantages over rivals. In short, these companies have acquired an influence that goes far beyond their market capacity. Khan and other North American scholars such as Lynn (2009) and Wu (2010) are called "New Brandeis movement", in reference to Louis Brandeis, who advocated in the first half of the twentieth century against oligarchs like John D. Rockefeller and J. P. Morgan. For this group, governments basically need to regulate big tech companies, as they did in past times with railroads, telecommunications, and energy sectors. Critiques of this group come from scholars such as Starr (2011) who argue that regulators oversimplify the cycles of economic expansion of industries, considering the picture of the moment instead of the longitudinal dynamics of the market evolution. In this view, regulators tend to adopt dichotomies between monopolies as dire empires and states as good regulators. All the same, today there is an absolute dominant operating system for computers (Microsoft), another for mobile phones (Android), a dominant search engine (Google), a hegemonic social network (Facebook), and a monopoly in the real market (Amazon). And even if new brands and companies emerge, especially from countries like China, the hegemonic proliferation of monopolies to process data would affect the very logic of the market and data subjects.

In that light, the discussion of restrictions to "big techs" is being conducted also in courts both in the United States and Europe. Since 2016, the European Commission is promoting the debate to tight regulation and has already imposed multi-million dollar fines, mainly against Google (three sanctions totaling 8.23 million euros)[123] based on antitrust legislation. Since 2017, the Commission has been investigating Amazon's business practices for alleged misuse of data from independent suppliers operating on its platform. Meanwhile, another front was opened in Europe to assure that technology companies pay taxes in the countries they operate ("Google Tax") despite threats of retaliation by the USA.[124] More recently, this issue has also been at the core of data transfers and protectionist trade wars between the biggest economies in the world, as powerful countries have adopted a neo-protectionist agendas, especially the USA and China.[125]

As alternatives to the issue of oligopolies, Cusumano, Gawer & Yoffie (2019) support a flexible system of oligopoly regulation analyzing each case separately. In their view, if it is possible to determine that a company inflates prices to weak

[123] Desjardins,… idem
[124] BBC News. 2019, July 11. 'France passes tax on tech giants despite US threats'. Retrieved from https://www.bbc.com/news/world-europe-48947922 in 01/22/2020.
[125] BBC News. 2019, May 10. 'Trade wars, Trump tariffs and protectionism explained'. Retrieved from https://www.bbc.com/news/world-43512098 in 01/23/2020.

other competitors, they believe that a group of legal experts must assess each situation to formulate the best answer to regulate antitrust policies. This capillary approach would be more efficient than passing rigid and universal laws that need to be constantly updated by law-makers. In a similar view, economists such as Sagers (2014) believe that fragmentation is a possible solution to restrain big techs that exercise questionable monopolies. But fragmentation, to him, should be conducted carefully to avoid the disproportional division of market sectors, the inhibition of competition, the lack of innovation, or what is worst, that the regulatory mechanisms have no effects or become ignored by the market. In another paper, Khan & Vaheesan (2017) explore the possibility of separating platform ownership from the commercial activity they host. Yet, the debate is still open to new ideas. Meanwhile, giant processors consolidate a hegemonic position that could be curtailed by market regulation. The forms and impact of those regulations are unknown, but they might happen, especially in regions where market-free supporters in North America, or market regulators in Continental Europe, had attained a traditional role to oversee oligopolies. Yet, one should see the continuous expansion of this market trend in the coming decades. In the long run, in our vision, regulators and companies would need to adapt themselves to new restrictions in terms of chains of supply, infrastructure constraints, and basic availability of resources/commodities to support the informational architecture of their empires. Moreover, new dilemmas would arise in the face of ecological changes and energetic transitions foreseen for this century.

Meanwhile, critical voices have existed to defend society from the role of giant corporations that promote a sort of "market fundamentalism". Those critiques are more incisive than the above voices and connect the role of big tech companies with the evolution of globalization or surveillance from a broader perspective. For example, Karl Polanyi in the classic *The Great Transformation* already highlighted market concentration as the activity that links the human experience with the dynamic to maximize the expansion of the fourth "fictional commodity". Polanyi's first three fictional commodities (land, labor, and money) were subjected to the law in previous eras. Although these laws have been imperfect, the institutions of labor law, environmental law, and banking law are regulatory frameworks intended to defend society (and nature, life, and exchange) from the worst excesses of raw "capitalism's destructive power" (Polanyi, 1944, p. 256). In his vision, economic capitalism's expropriation of human experience has faced no such impediments. More recent authors such as Shoshana Zubbof in *The age of Surveillance Capitalism* argue that right now we are at the beginning of a new arc that she calls information civilization, and it repeats the same dangerous arrogance from previous economic cycles of expansion. The aim now is not to dominate nature but rather human nature.

To Zubboff, surveillance instrumentarian power is opposite to totalitarian power. Instrumentarian recalls the utilitarian and plastic aspects in which people

become tools without violent and coherent schemes. To her, surveillance instrumentarian through corporations is intended as a bloodless coup. Instead of violence directed at our bodies, it operates more like a taming (Zuboff, 2019). Its solution to the increasingly clamorous demands for effective and productive life pivots on the gradual elimination of chaos, uncertainty, conflict, abnormality, and discord in favor of predictability, automatic regularity, transparency, confluence, persuasion, and pacification.

> We are expected to cede our authority, relax our concerns, quiet our voices, go with the flow, and submit to the technological visionaries whose wealth and power stand as assurance of their superior judgment. It is assumed that we will accede to a future of less personal control and more powerlessness, where new sources of inequality divide and subdue, where some of us are subjects and many are objects, some are stimulus and many are response (Zuboff, 2019, pp. 481-482).

Polanyi and Zuboff warn us against the excesses of market and the rampant data management exercised by powerful market players. Their visions are more critical but these need to be contrasted with the attempts of self-responsibility from the economic sector, the proposals to reform the market of data giants in North America and Europe, as well as the competition between market players among themselves and against states regulations. Through those lenses, the dynamics of governance in personal data business are far from being monolithic. Yet, we agree with them to identify the dominant position of big data players in their respective markets. Those players increase the concentration of information and economic power in data business and other economic arenas. To some extent, those corporations detain a hegemonic position in the international scenario that affects even our case studies. And that hegemony overlaps with structural or macro-political forces in the economic system. Not only because those players are as locomotives that transform the governance of data, but also the very capitalist pace and logic in the planet. More than a matter of revenues and numbers, the role of giant data corporations and their size in the market can be considered as a proof of their crucial role affecting the relationship between markets and governments, markets and users, technologies and humans, and humans and nature.

Epilogue

So far, we have expressed the main market strategies regarding the governance of personal data. Those aspects are summarized in Table 18. At this point, what are the overall accountability mechanisms and principles in this domain?

Both in Spain and Brazil, the accountable actors are small and big companies that obtain revenues through the processing and handling of personal data from citizens in their respective state/national territory or foreign countries (in the case of big companies). Those actors can be held accountable via direct and indirect means.

By direct means, companies are openly accountable to Data Protection Authorities (DPAs) in both countries. However, only recently, in 2018, this kind of accountability was reinforced in Spain and created in Brazil. Is too soon to assess and confirm if this mechanism will cover and turn accountable the constellation of companies in both countries via administrative regulation and sanctions (see the previous section). Furthermore, companies are accountable to enforcement authorities, such as security and intelligence agencies (Spain), and only to security agencies (Brazil), through administrative authorizations and judicial warrants. When big companies are accountable to enforcement authorities to transfer personal data, this channel can be enacted in four layers. As explained in this section,

1. The first layer regards the public frontend (visible and public content in websites) in which companies supervise themselves to monitor and delete certain information that violates their internal policies and legal rules (i.e. content related to hate speech, race discriminations, terrorism, etc.).
2. The second layer regards the private frontend (visible and private content in websites) that is monitored and altered by administrative and judicial requests of public authorities.
3. The third layer relates to the backend (technical operations to transmit or store data by companies such as internet processors and telecoms) at the metadata level. Metadata relates to “less” sensitive information such as log, name, address, IP, duration of calls, keywords, etc. This layer is disclosed to enforcement authorities under administrative requests.
4. The fourth and last one relates to the backend layer at the core data level. Core data relates to content and sensitive information like users’ emails, calls, video calls, messages, voice, images, etc. This layer is disclosed to enforcement authorities under judicial warrants.

By indirect means, companies are incidentally accountable to market regulators (such the European Commission on market regulations affecting companies like Facebook and Google, and the Consumer Protection Agency in Brazil), to third companies and certifiers (to obtain certificates of information security such as the ISO 27001 series), and to customers and users (in order to deliver efficient services and hold confidence to companies).

When companies are accountable to other actors by indirect means, they need to demonstrate that they abide by rules regarding transfers of data and information security safeguards (as demanded by data protection regulations), antitrust market practices (as in the case of market commissioners and regulatory agencies in the EU and Brazil), and transparent competitiveness and efficiency to deliver their services (i.e. to customers in the whole sense or to customers defense associations attached to market regulators, private and public).

In this section, we mentioned that companies are accountable through the elaboration of transparency reports that reflect the tip of the iceberg regarding enforcement authorities' requests to access personal data. Companies might also adopt privacy by design principles (PbD) following data protection recommendations. Furthermore, companies may turn their algorithms more transparent, auditing, and demonstrating their performance to external oversight without compromising industrial secrecy. Finally, they can support user center approaches in order to empower customers to exercise their data rights, correct misinformation, and enable mechanisms of co-creation and implementation of good practices. For example, surveys, communication channels, benchmarking of logistics, feedback of users can also be implemented to process personal data to customers or third companies, as in the cases of Facebook and Google. That process is behind the prosumer idea of personal data mentioned in the theoretical framework, in which producers of content become also consumers of refined information. In this cycle, personal data is collected, bounced, rendered, and returns to individuals as data doubles. Moreover, data is sold to third players to match correlations and find patterns of interest in commercial and security domains.

Table 18: Accountability strategies by market players.

Accountability dimensions	Cases	
	Spain	Brazil
Who is accountable?	Small and big companies processing and handling personal data of Spaniards to obtain revenues from this activity, either in Spain or in foreign territory.	Small and big companies processing and handling personal data of Spaniards to obtain revenues from this activity, either in Brazil or in foreign territory.
To whom are they accountable?	Direct means: • To data protection authorities. • To enforcement authorities Indirect means: • To market regulators • To third companies and certifiers • To customers and users	Direct means: • To the national data protection authority. • To enforcement authorities Indirect means: • To market regulators • To third companies and certifiers • To customers and users
About what are the services accountable?	Four layers of accountability to enforcement authorities (including intelligence services) 1. *In the public frontend layer, to monitor and delete information by default.* *2. In the private frontend layer, to monitor and delete information by default or under the pressure of authorities.* *3. In the backend layer, to deliver metadata under administrative request ("less" sensitive information of users)* *4. In the backend layer, to deliver content data level under judicial warrants (core and sensitive information of users)* Additional accountability forms to other actors: • About the transfers of data • Information security maintenance • Market practices • Customers' services.	Four layers of accountability to enforcement authorities (**except** intelligence services) 1. *In the public frontend layer, to monitor and delete information by default.* *2. In the private frontend layer, to monitor and delete information by default or under the pressure of authorities.* *3. In the backend layer, to deliver metadata under administrative request ("less" sensitive information of users)* *4. In the backend layer, to deliver content data level under judicial warrants (core and sensitive information of users)* Additional accountability forms to other actors: • About the transfers of data • Information security maintenance • Market practices • Customers' services.
How are they accountable? (measures)	• Elaborating transparency reports • Adopting privacy by design principles • Auditing algorithms • Supporting user-centered approaches	• Confectioning transparency reports • Adopting privacy by design principles • Auditing algorithms • Supporting user-centered approaches
Assessing accountability according to its internal principles	Did the accountability action result or promote at least one of the following principles? -Enforcement (sanctions)	Did the accountability action result or promote at least one of the following principles? - Enforcement (sanctions)

	-Transparency (passive) -Answerability (trust) ~~-Responsibility~~	-Transparency (passive) -Answerability (trust) ~~-Responsibility~~

Source: author

According to our methodological operationalization, the performance of accountability as a connector between authority and legitimacy is a matter of interest. When some authority is called to give an account, if that action does not entail more legitimacy, then accountability fails to reach its objective. As seen in the table, when market data processors handle and use individuals' data to obtain revenues and deliver products, accountability actions can spark enforcement, transparency, and answerability principles.

Public authorities, such as data protection agencies (DPAs) and security and justice bodies, can request the adoption of legal standards and the sharing of personal data by companies. In those cases, the companies have the role to mediate legitimacy insofar as individuals and public institutions are connected via market entities to enhance data rights and data governance. Moreover, public authorities can regulate the market, exercise pressure, and even punish market players. For example, administrative fines can be established in the field of personal data protection. Moreover, companies are obligated to share data if requested by enforcement authorities through administrative requests or judicial warrants. As this sections expressed, this provokes a relationship of cooperation but also of tensions and collisions between public authorities and market data processors (i.e. Google vs. the European Commission in 2017, and Facebook vs. the Brazilian courts in 2016, when the Brazilian Federal Police (PF) arrested Diego Dzodan, Facebook Vice President for Latin America.

As a form to turn the relationship with authorities more predictable, giant data processors like Google and Facebook started to release transparency reports in the last decade. Naturally, the reports enhance some degree of openness and visibility in this realm. The reports are important in order to elucidate the volume of requests and the capacity of states to request information from companies. However, companies still can adopt a bargain of power to release information according to their internal policies, such as intellectual property and industrial secrecy. For example, it is difficult to conclude if Facebook is being accountable by the information the corporation manages and releases (when enforcement agencies need specific data as proof for trials and judicial actions). In addition, Facebook might cooperate with public authorities by default, labeling this collaboration as "transparency." In any case, the transparency reports suggest that Spanish and Brazilian administrations have demanded data from foreign giant market processors through the four layers of accountability. However, it is evident that companies' transparency reports are only partially effective; while firms may modify their reports to present more information, these reports do not necessarily

induce changes in the procedures to handle data by industries and they do not induce the government to more broadly reveal its own activities (Parsons, 2019).

Despite data protection recommendations to establish proactive measures to process data, accountability and transparency used to be conducted in a passive form. That is, the openness to third players to obtain information security certificates (ISO 27000 and business certifications) and to audit algorithms, depend on the very initiative of companies to allow access to external supervisors. Companies like Facebook started to create an independent watchdog commission of prestigious practitioners and citizens to "moderate" users' content that cut across freedom of speech, ethics, and corporate governance.[126] Tweeter also started to check the reliability of tweets to assure compliance with internal rules, causing outrage from political figures that depend on this platform to convey unchecked messages.[127] However, those reforms are especially circumscribed to the frontend layers on the Web. In deeper layers, we mentioned that accountable algorithms, for example, still depend on an investigative journalistic culture to assess data sets, biases, and correct the correlations and uses of information. Given the proliferation of algorithms and data business, in public and market domains, more proactive and transparent measures need to be taken in the next decades addressing also backend layers.

In terms of transparency, companies have shown some degree of answerability to correct their practices. For example, when parliament commissions demanded explanations from Facebook after the Cambridge Analytics episode, the company promised to ensure better treatment of data and privacy.[128] As participation in public inquiries and sharing data with enforcement authorities is not enough to show improvement, companies started to support user-centered approaches to develop their products. By considering users as the main source of stability and reputation, companies like Facebook and Google, as well as telecoms, strived to promote trust among their customers. Trust became one of the main forms of currency to keep the confidence and to guarantee the supply of data subjects. As data companies depend on users to monetize benefits from their data (users are free products, producers, and consumers), trust assures that their business is protected. However, transparency and trust here are fostered in the side of the citizen (the watched), and neglected or ignored in the

[126] Lapowsky, I. 2020, May 6. 'How Facebook's oversight board could rewrite the rules of the entire internet'. *Protocol.com*, retrieved https://www.protocol.com/facebook-oversight-board-rules-of-the-internet from in 07/12/2020.

[127] Turley, J. 2020, May 28. Trump executive order retaliates against Twitter, but no one is defending free speech. USA Today, retrieved from https://eu.usatoday.com/story/opinion/2020/05/28/trump-takes-twitter-social-media-executive-order-free-speech-column/5278725002/ in 07/17/2020

[128] Google and Facebook learned to weather these storms with the so-called the "dispossession cycle," and close observation of this new crisis suggested that a fresh cycle was in full throttle. "As the threat of regulatory oversight grew, the adaptation phase of the cycle set in with a vengeance. There were public apologies, acts of contrition, attempts at mollification, and appearances before the US Congress and the EU Parliament" (Zuboff, 2019, p. 477).

side of strong data processors from the market (the watchers). In that sense, the metaphor of "slides of visibility" (Bakir & McStay, 2015) explained in the previous section is useful again to criticize transparency schemes in the governance of personal data, including the role of market processors. In the current scheme, users are transparent to data processors such as Facebook, but the reversal is not true. Companies became friendly and trustworthy platforms, but little transparency (aside from user setting tools and overall guidelines shared by default) exists from data processors to users.

Finally, when it comes to the principle of responsibility, the ability to fulfill missions and duties, many obstacles can emerge despite the good intentions of market players. Responsibility increases as the market follow accountable practices and standards (see the last table) to manage personal data. However, one question that remains is to what extent companies are responsible before the public, customers, public authorities, and private stakeholders when they handle data. As complex companies are responsible for so many fronts, being accountable to everybody could mean being accountable to 'nobody'. Amidst the intersections of international and local regulations, the pressure of the public (in terms of social and environmental responsibility), the pressure of enforcement agencies to share data, the pressure of competitors, and the pressure from shareholders to obtain revenues, giant data processors tend to manage their multiple mechanisms of accountability in favor of also powerful players (public authorities and market shareholders). The transparency reports evidence that companies seek to standardize the relationship with enforcement and public authorities. But this puts the role of citizens to shape their business in a position of mere customers and users. In that sense, we can express that responsibility, as a principle of accountability, exists in the market domain but it tends to become fuzzy and diffuse. In that sense, responsibility and its precise extension are still debatable. Perhaps this is the main weakness of business models handling important elements like privacy and personal information as major sources that sustain their functioning. In a multiple accountability regime, the commodification of users' data is still the cornerstone of this realm.

Yet, if data processors work with refined information extracted from raw personal data, this performance should not be similar to companies that control natural commodities. Processors should avoid indifferent approaches, meaning that it does not matter what is in the pipelines of data as long as these are full and flowing. Data processors can foster accountability principles by promoting "good" practices and standards. Besides, they can foster innovative forms to protect and transfer data to fuel their activities. We will revisit the data economy and new missions for companies in Part 4. In the next section, we will see that the civil society has also a role in the governance of personal data.

5.3. Civic agency

So far, we have seen the governance of personal data in two fronts: state regulations and market practices. Yet, some areas remained untouched. Thus, we now focus on a third domain: civic agency. Agency means to pass from a passive role to an active one in order to obtain power or decide as a sovereign actor. Hence, this section exhibits the tactics, operations, and strategies of the general citizenry to obtain more power and promote accountability by different means and purposes. Here, we show why the citizenry mobilizes to redefine and contest the management of personal data, and the strategies they use to exercise this mobilization.

Why people engage against the "normal" use of their data? Why contest the governance of personal data on the Web and beyond? This idea of non-conformity leads us to readdress the basic notion of resistance and surveillance.

Surveillance, as explained before, is more than the simple use of data and the categorization of persons. It is also related to power relations and real impacts on people. Surveillance entails representation and technology. Acknowledging how surveillance technologies can represent data collected at source or gathered from another technological medium is a first step to understand resistance. As the representation and use of technology entail "meaning", some people can challenge the identification and the meanings produced by data processors. Regulations and market practices allow some degree of a bargain to correct/contest the meaning and representation of personal data. Yet, resistance can disagree with those channels and promote ulterior struggles. This is especially true if we consider the commodification of personal data and the limits of institutional accountability mechanisms. In that sense, people can feel they are manipulated/sorted/categorized/labeled by dispositives that produce different versions of life as lived by surveilled subjects. In that sense, power relations are evident as watching groups can regulate the flow of information and knowledge about surveilled subjects. Resistance then can be conceptualized as "breaking or disrupting those flows and creating spatio-temporal gaps between watcher and watched" (Ball, 2005, p. 89).

As resistance is a relational concept, Ball (2005) reveals two inherent assumptions here: (a) the subordinate actor is an autonomous agent capable of interacting with both technologies and observers, and (b) resistance emerges because surveillance is recognized and rejected as abnormal and unnatural. Other scholars, like Mann, Nolan & Wellman (in Marx G., 2003) propose 'sousveillance' as a counter form to surveillance. Sousveillance uses technology to confront bureaucratic organizations by inverting the gaze toward the watchers or

surveillance authority, resisting surveillance through non-compliance and interference; blocking, distorting, masking, refusing, and counter-surveilling.

Who resists? What groups and organizations resist to the management of personal data by institutional and market domains? To answer this question, we need to look at the social domain that remained outside the state-forms and market in this study: the civic agency. In rough terms, civic agency means "we the people". It means the citizenry united under certain circumstances and motivations. In that sense, the term civic agency has been very elusive and vague to be put into a single definition. Yet, this agency presents some basic features related to motivations, strategies of association, temporality, and purposes (Emirbayer & Mische, 1998) (Dagnino, 2008). The theory of civic agency has addressed practices (rational, phenomenological, communicative), relations and engagement with (or against) the social structure (i.e. against hegemonic groups and players). Moreover, it has been described as a crucial analytical component for "charting varying degrees of maneuverability, inventiveness, and reflective choice shown by collective people in relation to the constraining and enabling contexts of action" (Emirbayer & Mische, 1998, p. 3). Pragmatic theorists have rejected the dualist division between space (structure) and time (of association) and between utilitarian strategies and motivation purposes, arguing that both sides are always connected and change according to the ongoing process of creating agent citizens in a contingent context (Joas, 1996).

From a governance perspective, "civic agency is the shift that involves a move from citizens as simply voters, volunteers, and consumers to citizens as problem solvers and co-creators of public goods; and from democracy as elections to a democratic society" (Boyte, 2005, p. 6). Such a shift has the potential to address public problems and promote the commonwealth. Moreover, achieving this shift requires deepening the civic, horizontal, pluralist, and productive dimensions of politics. To achieve those values, the civic agency is leveled by the multifaceted and pluralistic interactions comprised of active social players that are especially located outside traditional forms of government and market. In the digital realm, the civic agency could coalesce users' interactions and communications with different purposes. For example,

> Online civic and political agency is less likely to advocate a single ideological position (although they sometimes do) than reflect a set of values, experiences, and reflexive disclosures of identity […]. Governments prefer to deal with settled public interests expressed as aggregate demands than informal collectivities working towards a common identity through mutual disclosure. Those who are active within civic and political networks do not necessarily know what they demand: they are searching for articulations of their interest through a process of ongoing production of and exposure to new knowledge (Coleman & Blumler, 2009, pág. 135).

Because of the diffuse and decentralized characteristics, the civic agency can be associated in rough terms with the “crowd of people” or the “multitude”. The multitude is a concept that represents the social multiplicity of subjects that is able to act as a common agent of biopolitical production within the political system. In the European Modern Age, the notion of “multitude”, promoted by Spinoza, differed from the distinction of "crowd", promoted by Hobbes. The basic difference is that, in the distinction of Hobbes, the group of citizens is simplified to a unit as a single body with a single will, either a mere crowd or mass that meets the necessary requirements to be considered as people. For example, the very idea of State was born of a single authorization of sovereignty by a general idea of people (see Chapter 1). In turn, the Spinozian multitude concept refuses that unity retaining its multiple nature (Virno, 2003). In this sense, the decentralized characteristics of the Web can be promoted by the multiple fronts of the civic agency as the multitude. In simple terms, through network relations established in the digital era, resistance work as a multitude, not as a simple entity or mere people (Hardt & Negri, 2004).

At the crossroads of globalization, due to the colonial, economic and historical heritage, the concept of multitude in Latin America unfolds in particular subaltern subjects that many times are overlooked by the modernization of European matrix. In that sense, it is necessary to be careful to transpose the concept of the multitude to other regions. For example, in the economic history of Latin America, paradoxically, one invisible subject had also claimed to have a voice: the economic entrepreneur rooted on familiar traditions. This subject has been associated as part of the elite, by the promotion of inequalities in Latin America, and by the links with transnational capital (Stiglitz, 1986). Yet, this subject, in the small and intermedium scale, is just one of the transdisciplinary groups that demand new epistemological status, where family organizations, informal markets, and migratory networks replace the imperfect labor market and definition of the multitude as in Global North. Santamaría García (2019) argues that most of the entrepreneurs in Latin America are small and medium informal businessmen, not oligarchs. The multitude, therefore, goes beyond the mere differentiation between progressive and conservative forces. Yet, it could be related to the groups from the “bottom” that depend or react against those located at the “top” of the social stratification. Even in that perspective, relations are multiple and not fixed.

The multitude contesting the rulers of globalization, for example, is a particular phenomenon raised at the beginning of this century. Between 2001-2003, at the juncture that goes from the end of the so-called Cycle of Counter-Summits (Seattle 1999, Genoa 2001) and the Global Campaign against the war in Iraq, networks of thought and action were articulated in cities around the world, including Spain and Brazil. Part of the network worked with new media, using the Internet, experimenting with technologies and integrating the hacktivist-hacker movement that emerged in those years. The amalgam between the use of digital

networks and the multitude was deepened in the next decades until the point in which,

> From the traditional Emitter-Message-Receiver scheme, we have moved to a complex map of a multitude of emitters that, at the same time, are formed as receivers, in the new collaborative construction of meta-narratives. These narratives do not have to coincide (in fact they do not) with the institutional narrative that has been reproduced from the spheres of power through their means of communication to shape reality (Toret J. , 2012, p. 10).

The array of social interactions and interests as attested by the quotation inhibits an absolute conceptualization and ultimate orientation to the civic agency. Yet, when it comes to promoting accountability, one major concern is whether this domain could really promote major changes in politics, such as to replenish the position of civic actors to demand more horizontal governance and mitigate the instrumentarian power of surveillance and the commodification of data subjects. A real connection between accountability and civic society still poses a real challenge, especially when it comes to counteracting hegemonic players that use to deal with restricted groups and voices to solve public problems. Thus, to answer those dilemmas, we need to analyze resistance strategies and the potentialities of the civic agency.

In terms of resistance, what kind of civic agency operations and strategies exist? A binary definition of the civic agency would be to categorize formal/informal strategies, legal/illegal tactics, and offline/online actors. However, this division is poor and overlooks many components and reasons that sustain resistance from the civic agency. For instance, it ignores the amalgam between the internet and offline tactics, and the problem of delimiting legitimate resistance to those practices that only abide by the law and legal rules (not always legality is legitimate, nor every illegal practice is illegitimate). Thus, we propose four operations or streams to categorize resistance:

- Ironic stream (communication)
- Deliberative stream (cooperation)
- Agonistic stream (confrontation)
- Despair stream (conflict)

5.3.a. Ironic stream

The Ironic stream is related to the dimension of communication and narrative. Politics is narration, storytelling, and sharing/struggling a vision of the world. In the theoretical foundations of this work, we mentioned that exceptional politics are not disconnected from normal ones. Exceptionality is connected to governmentality tools or dispositives that "normalize" human actions. Since every political decision has a degree of exceptionality, even in the infinitesimal scale of analysis, then there is always room for leeway, re-creations, and absurdity. In that sense, every act is exceptional (see section 1.2) in some degree as it is permeated by non-common or expected factors. Even life and the mere fact of existing implies in being embraced by absurdity and exceptional conditions that re-direct our lives. In that sense, life and the mere existence of people is resistance. To be born implies in a continuous act of resistance (in physical, psychological, and political terms) between the human being and the environment. In the infinitesimal scale of resistance, even breathing and getting older is to resist life and endure against the outside world. This absurdity, the burden of life related to resistance, can be labeled as the ironic stream. "When you realize how perfect everything is, you will tilt your head back and laugh at the sky", a phrase attributed to Siddhartha Gautama or the Buddha, exemplifies that even the most patient and perseverant human recognizes that, sometimes, the inner-self just need to adapt itself to the environment. It shows that existence is navigating with(out) a compass to synchronize our "nothingness" with the external world.

In the ironic stream, as we live in a condition of absurdity and endurance, this scale of resistance relates to the re-presentation of the surrounding world and ourselves. This stream relates to communication and the construction of narratives.[129] Even religion has an important role here. To endure the absurdity of

[129] This idea is different from the famous *ironist* concept formulated by Rorty (1989). To him, ironist is the sort of person who faces up to the contingency of his or her most central beliefs and desires. Rorty argues that all language is contingent: truth or falsity is not determined by any intrinsic property of the world being described. Instead they purely belong to the human realm of description and language. In his ironic model, people would never discuss restrictive metaphysical generalities such as "good", "moral", or "human nature", but would be allowed to communicate freely with each other on entirely subjective terms as long as they can coexist. Since then, Rortian irony became a target of criticisms that see it as marred by the conflict between skeptical distance and commitment. But such critique ignores the fact that Rortian irony belongs to broader literary intuition in the interpretive game between formal, cognitive, and aesthetic coherence of literary texts as a potentiality to be realized by readers. Rorty transposed this equivalent to the practices by which inhabitants of democracies reexamine and recompose the materials of their networks of beliefs. Since such practices require a combination of ironic distance to the examined materials with a commitment to the interpretive process itself, Rortian model of irony could be labelled as a "method" of approximation to social objects based on the analysis of texts (Bartczak, 2015). Whereas, our ironic model is a strategy that comprises tropes of language, plots, and feelings (like humor) that go beyond literary mechanisms to encompass communication as an independent mediation stream to promote social changes, even if those changes remain in the dimension of language itself.

life during human history, religion raised not only as a ritual of dogmas but also as a social-communicative action. Even nowadays, religion, among many connotations, also entails a narrative to tackle intangible problems. Comforting words such as eternal life, salvation, paradise, illumination, and hope are more than words. They were also the story of resisting and giving a sense to the human condition in the last millennia.

But in the world between humans, in politics, the first stream of resistance corresponds to how we communicate and bond with other persons. Here, language, rhetoric, argumentation are as important as sensations, feelings, and arts. However, compared to other forms of language and feelings, humor represents subtle or direct transgression. Humor is by nature confrontational. To laugh at something means to deal with absurdity. In fact, sometimes a joke can be funnier just because we do not know if it is okay to laugh at something or not (Weems, 2014). In addition, the fact that a joke bothers some groups can spread the irony and humor even more. When surveillance of the Spanish dictatorship depleted the formal resistance in the streets after the Civil War, establishing censorship across culture and arts, one of the last tools of resistance was the hidden use of jokes and irony to represent the Caudillo (García & Tauste, 2006). In terms of structure, jokes and rhetoric have some real effects. However, they did not cause the fall of dictators. No joke overthrew Franco and that Nazis were defeated by a World War, not by humorous comment. Yet, in terms of agency, ironic narratives were very present and helped to undermine the regimes. In another example, one Turkish joke tells that a prisoner goes to the prison library asking for a specific book; the guard then says: "we don't have that book... but we do have the author."[130] When we read this example, we can agree (or not) that this is funny. Yet, it can help to lead with the absurdity of overwhelming conditions of oppression.

Let us consider some tactics in this stream that connect aesthetics, rhetoric and different tropes such as humor and irony. In 2017, the Spanish Audience Court sentenced Cassandra Vera to one year in prison due to humorous internet memes on Twitter about Luis Carrero Blanco, the Francoist President killed by ETA in 1973. At that time, the Court alleged hate-crimes and humiliation of victims of terrorism, but Cassandra described the sentence as "absolutely absurd and stupid".[131] In 2019, The Spanish Supreme Court annulled the sentence expressing that "the repetition of easy jokes about Carrero Blanco is socially and morally reprehensible as a mockery of serious human tragedy, but no criminal sanction is

[130] Temkin, M. 2018, August 24. Twitter post, retrieved from https://twitter.com/moshik_temkin/status/1033031762094579712?ref_src=twsrc%5Etfw in 02/04/2020.

[131] Ángel Méndez, M. 2017, March 29. ''Caso Cassandra': un ridículo jurídico nacional (que se convertirá en internacional)'. *El Confidencial*, opinión. From https://blogs.elconfidencial.com/tecnologia/homepage/2017-03-29/cassandra-vera-carrero-blanco-audiencia-nacional-twitter-prision_1357648/, accessed in 02/05/2020.

to be provided."[132] In short, digital memes conveying irony, sarcasm, and other narrations spread very quickly and are useful tools to corrode the normalization of social practices across many cultures (Hristova, 2014; Lee & King, 2015; Soh, 2020; Yang & Jiang, 2015).

Another tactic consists of merging aesthetics and resistance. In Brazil, one example is the story of Rennan da Penha, a carioca funk DJ who helped to create one of the biggest informal music festivals in favelas of Rio de Janeiro (Baile da Gaiola). The festival convoked around 10,000 people on weekends and influenced other music producers that became viral on the Web, like *Turma do Pagode* and *Nego do Borel* who have more than 200 million views on YouTube. In January 2019, Rennan da Penha was arrested on charges of association for drug trafficking. He was accused of participating in events promoted by criminals in local communities and for publishing content endorsing violence and armed gangs. He was acquitted of the charges at first instance, but after an appeal by the local Attorney Office, Rennan was sentenced to 6 years of prison. The judge of the case stated that Rennan had the role of criminal "vigilante", as he reported "the tactical movement of the police in favelas sending WhatsApp messages." Rennan's defense presented habeas corpus with the Supreme Court, expressing that his messages were not proof to associate him with violent gangs.[133] We cannot access Rennan's messages to prove his innocence. Yet, the favelas festivals and his influence became even more popular as a form of expression by excluded population; a way to give visibility and a form of subtle resistance against many illegitimate police operations that produced violence and arbitrary detentions. Urban aesthetics and popular narration through funk music might not be directed to defy the establishment. Yet, this music can help to reshape cultural codes and communication in the hands of excluded population (Sneed, 2008).

To close this subsection, the way we establish narratives, stories, and contexts to communicate and resist also matters directly in the realm of personal data. Here, the capacity to critically understand and control one's data is now a crucial part of living in contemporary society. In this sense, traditional concerns over supporting the development of 'digital literacy' are now being usurped by concerns over citizens' 'data literacies'. In this logic, Pangrazio & Selwyn (2019) affirm that, alongside the use of tactics to process data, data understandings and data reflexivity are crucial nowadays. That is, basic resistance actions also require a basic notion of what is happening to our data. Thus, in the same logic reading and writing were the first tool for emancipation and liberty throughout history, today,

[132] Pérez, J.; Torrús, A. 2018, March 1st. 'El Tribunal Supremo absuelve por unanimidad a Cassandra por los chistes de Carrero Blanco'. *Público*. Retrieved from https://www.publico.es/sociedad/cassandra-absuelta-supremo.html in 02/06/2020.

[133] Zuazo, P.; Guimarães, H. 2019, March 22. 'Justiça manda prender DJ Rennan da Penha, idealizador do 'Baile da Gaiola', por associação para o tráfico'. *Extra*. Globo. Retrieved from https://extra.globo.com/casos-de-policia/justica-manda-prender-dj-rennan-da-penha-idealizador-do-baile-da-gaiola-por-associacao-para-trafico-23543633.html in 02/06/2020.

those authors support the widespread development of personal data understanding and agency across general populations. It makes sense to look back to pre-digital forms of critical literacy development, and use these established notions of literacy as a basis for working out realistic ways of supporting the capacity of individual users to engage with seemingly imperceptible personal data infrastructures and data economies. In short, personal data literacy can be developed as a critical pedagogical effort to reshape data representation and communication, and so the material opportunities and social roles for individuals.

5.3.b. Deliberative stream

The deliberative stream refers to resistance as cooperation. In the deliberative stream, to foster more accountable governance, some scholars have suggested counterbalancing hegemonic practices on the Web by cooperation at micro and macro levels. Based on the deliberative theory of communication (see section 1.3 in Chapter 1), their supporters value "Not agonism, but agreement/disagreement underpinned by reciprocity […], not an articulation of social movements, but free association and affiliation" (Hands, 2007, p. 91). In this stream, the aim is to join cooperation, deliberation, and add forces. To this logic, the production and the consumption of data can be processed in a world where users, workers, consumers, and other people can cooperate through digital forums, reinforcing the struggle of traditional association, from free and sporadic thematic groups to social movements and labor unions. Digitalization, in a more progressive perspective, raises the opportunity of a connected movement to create "a transnational association of consumers/workers" (Karatani, 2005, p. 295). Yet, we believe that this association must not neglect that the line between workers and consumers has been blurred as a result of the "prosumer" alienation and commodification of personal data, as stated in the theoretical framework. To resist those trends, association and cooperation in the deliberative stream can adopt many tactics.

The tactics in the deliberative stream can be performed either by institutionalized or by informal forms of resistance. One institutionalized example is the model in which The Internet Corporation for Assigned Names and Numbers (ICANN) has employed. Although jeopardized by stronger economic voices and its implicit allegiance to USA law, the ICANN adopted a participatory line of open public comment before policymaking. The ICANN has institutionalized mechanisms of review with constant deliberation to introduce reforms and to manage the governance of websites and addresses (Malcolm, 2008)(Malcolm, 2008). If the Internet is a place with many "roads" and "streets", the ICANN gives the name and the address to navigate and find any virtual location. It has the power to map the virtual world, allowing web users to index and to find websites. On the other hand, cases of informal or not permanent organizations are plenty. A strong civil society lying outside the power of stronger players is important to

influence public accountability. An independent sphere can promote answerability (i.e. after the misuse of personal data) or spark enforcement (like pressing justice courts to take actions over the misuse of personal data). For example, spontaneous associations for civil rights initially fostered the judicial clashes that raised discussions incorporated in the current European Data Protection Rules, such as "Digital Rights Ireland" and "Google vs. the Spanish Data Protection Agency (AEPD)" in 2014.

One example of a tactic employed by the amorphous cyber multitude is hacking. Despite their several categories (novices, cyber-punks, ethical hackers, hacktivists, crackers, insiders, criminals, and government agents), hacking has the potential to either undermine or engage with accountability principles. In the last sense, Jordan (Jordan, 2007) identifies Digitally correct hacktivism as a group that promotes the right to freely and securely access digital content. In Spain and Brazil, this group can be connected to notable activist communities like WikiLeaks, Anonymous, and LulzSec as they use sophisticated tactics like remote controlling, code programming, and vigilance of government action in the cyberspace to guarantee open access to information on the Web. Hacking can promote tactics of confrontation, but its commitment to the access of information allows especial potential in the deliberative stream. In that logic, we argue that free and secure tactics to facilitate access to the Internet can be considered as accountability strategies. Despite the distance from Schedler and O'Donnell's accountability concepts, those tactics can diminish the power asymmetry between data subjects and data processors. For instance, hacktivism has a clear potential to avoid the collapse of digital information into a de-facto monopoly of domination managed by powerful state and commercial players. In that sense, many of the scholar references for this study were obtained thanks to hacking websites that ensured free and universal access to academic content that otherwise would be closed or paid.[134] Without this action, this and many studies in the world would be compromised in their potential and range. In the academic world, some studies even affirm that open access does not compromise publishing editors and paid content. Rather, it helps to canonize magazines and increase their reference impact (Priego, 2016). In the end, this mechanism does not demolish the traditional publishing system nor is the heroic 'Robin Hood tactic' to promote free access.

Meanwhile, in other domains, Digital correct hacktivists supporting Open Codes are behind common applications and software. Open Codes are free and public and they are being used to preserve decentralized informational architectures, such as Blockchain databases, to develop Smartphone applications,

[134] For instance, Sci-Hub is a search engine for academic works founded by Alexandra Elbakyan in 2011 in Kazakhstan in response to the high cost of research papers behind paywalls. Sci-Hub and Elbakyan were sued twice for copyright infringement in the United States in 2015 and 2017, and lost both cases, leading to loss of some of its Internet domain names. The site has cycled through different domain names since then.

such as mobile operative systems, and to develop efficient Privacy Enabling Technologies (PETs) that inhibit intrusive surveillance activities. It can be said that no one who uses computers, smartphones, or the Internet today spends a single day without using free software. Almost all paid programs and applications are based on fragments or entire programming based on open codes. People use these apps even without knowing it; whether accessing servers, operating systems such as Linux or Android (only in its core functions), or in online applications. The Tor project (The Onion Router), for example, has fragments of open code to allow anonymous navigation on the Internet. This allows that the consulted information can travel through different intermediate stations before reaching a destination. The tool has proved useful in cases of government control. Also, if users complement it with other security measures such as connection to a proxy, it is difficult to know whether a particular computer is requesting information from a censored space. This happened in 2009 in Iran with the Saudi website Tomaar, as documented by Morozov (2013). It has been said that Tor is correlated with illegal and criminal activities on the Web. However, the correlation has not been proved (Monk, 2017). Indeed, Tor allows virtual spaces that are more difficult to be reached by enforcement agencies, but niches in this domain could be monitored by target surveillance "patrols" and eventually uncovered by mass surveillance programs (Feigenbaum & Ford, 2015). This is because no anonymous communication system can succeed if other software the user is running gives away his/her network location.

On the other hand, as resistance always interplays with counter-resistance, many private companies have found an interest in an open and free source as it facilitates external contributions to their projects and the omission of a license to use the programs (Lerner & Triole, 2002). This is the case of Google or Amazon, which have various open software projects, as well as servers and multiple services that run under free programming languages and operating systems. Likewise, other companies related to telecommunications and electronics release their code as part of their business strategy. IBM, which owns Red Hat, also uses free software for strategic reasons and as a competitive alternative to companies that use proprietary code. Thus, although free software presents an alternative to the logic of copyright and commodification, it is not a space that is wholly independent of corporate control insofar as it can be used by commercial organizations with goals that are different from the original ones proposed by the hacker communities (Levy S. , 1994).

Notwithstanding, in this stream, one can find several billion users a day, and a community of millions of developers, programmers, and managers distributed globally. In addition, commercial software does not allow technical audits at the same rhythm as the ones implemented by public forums. Therefore, commercial software is often exploited by security agencies to attack systems or implement backdoors as expressed by WikiLeaks cable Vault 7 that revealed CIA hacking

tools.[135] But not only security agencies can exploit software vulnerabilities. The WannaCry cyberattack of 2018 in Spain, for example, exploited security vulnerabilities of commercialized programs that were not updated to the later versions.[136] As the Internet and software practitioners and scholars often point out, cooperation has many advantages in this domain. Access to the common in the network environment represents access to "common knowledge, common codes, common communication that [in turn] is essential for creativity and growth" (Hardt & Negri, 2009, p. 282) of a society shaped by common ownership and co-operative production.

Beyond market data processors, there is a world of autonomous social networks (RSAA). Although not as popular as Facebook and Google, RSAAs are based on collaborative principles, participatory and horizontal relations that oppose the commodification of data. This is the case of N-1, Rise up, Diaspora, and Identi.ca, which do not profit from the management and exploitation of data. N-1 resembles the notion used by Deleuze & Guattari (1988) in *A Thousand Plateaus*. To explain the Rhizome, those authors affirmed that N-1 is the multiplicity not reducible to "One". It is the subtraction that allows multiplication (Toret J. , 2012). In the idea of the social network, N-1 became a fundamental network for many of the 15-M Spanish manifestation movements on the Internet. According to its original intention, N-1 is presented as an alternative or complement to commercial social networks. In turn, Diaspora presents itself as an alternative to Facebook. Diaspora is a decentralized social network as the user´s information does not pass through the servers of a company. Users can upload information to servers of their choice, or pods, in which data is supposed not to be saved or stored permanently. In addition, Twister is a P2P (peer-to-peer) microblogging network fully decentralized. In this network, each user is a node. Photos, status updates, data, etc., are everywhere and nowhere because they are scattered throughout a network where each computer stores information locally. There is no censorship and it has a messaging system (Direct-messages) encrypted between the sender and the receiver (end-to-end system). Finally, DuckDuckGo (DDG) is an internet search engine that emphasizes protecting searchers' privacy and avoids the filter bubble of personalized search results. DuckDuckGo distinguishes itself from other search engines by not profiling its users and by showing all users the same search results for a given search term. Some of DuckDuckGo's source code is free software under the Apache 2.0 License (a permissive free software license), but the core code is patented.

---

[135] *WikiLeaks*. 2017, March 7. 'Vault 7: CIA Hacking Tools Revealed'. Press release. Retrieved from https://wikileaks.org/ciav7p1/ in 02/07/2020.

[136] Palazuelos, F. 2017, May 19. 'How the WannaCry ransomware attack affected businesses in Spain'. *El País*. Cybersecrutiy. Retrieved from https://english.elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html in 02/07/2020.

Another example of deliberative tactic is “Democracia 4.0”. This is a legal initiative that aimed to promote and implement an electronic voting system by the digital signature in the Spanish Parliament since 2012. Based on article 1.2 of the Spanish Constitution, “National sovereignty comes from the Spanish people, from which the powers of the State emanate”, the platform is also based on Public Administration law to accelerate deliberation on Legislative bodies and eliminate procedures that hamper electronic votes. The project supports the idea “one citizen, one vote” instead of the constant mediation of Parliament members. The project was never implemented at the state level, but it has other possibilities such as the combination with popular legislative initiatives also enshrined in the Constitution. In that hypothetical scenario, once presented in Congress, a Popular Legislative Initiative (ILP) would require the direct participation of the people via electronic forums with digital signatures (Gilabert, 2013). Those initiatives would then be transferred and weighted in the Delegate Commission of the Congress, which must decide the inclusion of the ILP in the plenary session of the Houses. Yet, broader technological access to overcome Internet gaps and deeper changes in the legislative process is needed to implement ILPs in the Legislative process.

The combination of popular initiatives with open consultation has also reinforced the agency of citizens in government policies. We mentioned that the Brazilian Internet Framework (Marco Civil) of 2014 ensured principles of universality, neutrality, and decentralization of the World Wide Web. This document was a product from the commitment of Internet activists, social movement, and even companies and public organizations. From the human rights perspective, many goals - especially related to greater social inclusion, freedom of expression, and fostering a digital culture - can be considered as achievements in the Framework. Yet, this document must be understood as a guideline to future legislation in Brazil. In turn, the Spanish government made a public consult to construct a Chart of Digital Rights in 2020. Despite civic agency groups had less involvement and time to coproduce this document if compared to the Brazilian Framework, the Chart reinforced the right to Internet neutrality. Also, its ambitious scopes include rights to cope with artificial intelligence. For example, it guarantees the right to no discrimination in decisions based on algorithms. Moreover, it mentions rights in the use of neuronal technologies. In this case, the aim is to preserve self-determination, ensuring the confidentiality and security of brain data. Yet, it is unclear to express how the Chart will be implemented. At this moment, it is a guiding document that aims to define the evolution of digital rights.

5.3.c. Agonistic stream

The agonistic stream consists of challenging hegemonic players by promoting the "necessary confrontation". This stream is based on feminist and poststructuralist approaches to whom deliberative approaches ignore communicative 'distortions' (and exclusions) resulting from coercion, instrumental-strategic action, social inequalities, and technical limitations. Because of those distortions, this perspective tries to emphasize agonistic features (the necessary conflict) to construct new interactions on the Web. Agonistic notions highlight the antagonisms between different agents and groups to redefine power asymmetries through digital strategies, such as hacking. In other words, this perspective privileges awareness and responses stemmed from struggle and resistance to coalesce civic agency groups.

In the agonistic perspective,

> Technopolitics is not "clicktivism," that is, it is not simply the new culture of engagement based on click, a kind of digital goodness. A social change will not come by doing many "likes" or an online petition. Thousands of events on Facebook, or campaigns on the network, fail for multiple reasons, but mainly because they have a simplistic understanding or voluntary activism on the network. Thus, they do not open any prospect of social change. We believe that there is a growth of a dangerous mix between social volunteering and conversion of the third sector that speaks of cyberactivism or digital participation and which is at the antipodes of the transformative potential of the strategic use of digital networks and identities for collective action (Alcazan, Axebra, Levi, SuNotissima, & Toret, 2012, p. 42).

As a tactic in this stream, scholars like Jordan (2007) identifies the role of "Mass action hacktivism". For Jordan, "Mass action hacktivism puts radical democracy at the center of their aspirations, whereas digitally correct hacktivism's deep concern for free, secure access to all information, focuses them towards the infrastructure of information" (Jordan, 2007, p. 75). Mass action hacktivism also focuses on political legitimacy and is closely related to communities that support alter-globalization and global justice movements like Independent Media Watchers, Ecologists Groups, "Indignados" Movement, Occupy Madrid, Movimento Passe Livre, as well as platforms who belong to the European and World Social Forums (Schlembach, 2016). In the agonistic stream, many of the struggles and social movements are updated in the digital world to demand political changes in which the electronic interfaces encounter material infrastructures and biological bodies.

Regarding other tactics, one can mention struggles over data such as Distributed Denial of Service attacks (DDoS) and encryption technologies, which can also be used reshape the use of personal data and. One example was the platform *Stopdesahucios*[137] (Stop evictions) designed to identify, map, and follow the evolution of evictions in Spain. The tool unifies free software, especially OpenStreetMap, an open project similar to GoogleMaps, and Ushahidi, mapping software for disaster or conflict zones. Both tools allow the register of evictions, enabling actions to stop them or helping evicted families as well as to follow the consequences of those interventions. It was created to help the group People Affected by the Mortgage (*Personas Afectadas por la Hipoteca*, PAH), which emerged in 2011 to monitor housing policies and evictions in Spain. Stopdesahucios was produced by Hacksol, the AcampadaSol group of hackers (who supported the occupy movement in Madrid that year). After the expansion and coordination of those collective actions, the group became "15hack".

In Brazil, during the protests of 2013, Anonymous Brazil conducted DDoS attacks against institutional and government websites. The group was accused of "digital vandalism" at that time, yet, they took part of the riots against the rise of transportation tickets and the group was one of the "driving forces" of the protests, coordinating marches and sharing content with millions of followers, from memes to social manifestos.[138] The organization also carried out DDoS attacks against the Australian Government's control of information (Operation Titstorm) and PayPal (Operation PayBack) when this company prevented WikiLeaks from using its payment gateway for donations.

As another agonistic tactic, we also can consider the role of whistleblowers who challenge formal institutions and even entire governments. The most famous digital leaks on national security issues that affected Europe and Brazil in 2013 resulted from a level of commitment against the indiscriminate use of information to sort, categorize, discriminate, and stigmatize people based on the collection of personal data. For instance, as seen in Chapter 3, WikiLeaks demands mainly the transparency of the state, while it demands the privacy of its internal and financial functioning. WikiLeaks has also been accused of fraud, espionage, and conspiracy against the United States. As a form of indirect pressure, Chelsea Manning was convicted by a military tribunal for the leaks about the collateral killing and revelation of documents about the war in Afghanistan. WikiLeaks leader, Julien Assange, on the other hand, was accused in 2010 of statutory rape and sexual harassment. In April 2019, his asylum in the Ecuadorian embassy in London was withdrawn following a series of disputes and his arrest and sentenced to 50 weeks

[137] Retrieved from: http://stopdesahucios.tomalaplaza.net/ in 02/08/2020.
[138] *Anonymous Brazil,* 10/21/2015, 'O alcance das manifestações em 2013 na web chegou a mais de 600 milhões de internautas, com uma quase unanimidade a favor dos protestos'. Retrieved from https://www.anonymousbr4sil.net/2015/10/o-alcance-das-manifestacoes-em-2013-na.html in 02/10/2020.

in prison in the United Kingdom. In Chapter 3 we mentioned that leaking for the sake of leaking is misleading and organizations such as WikiLeaks have limitations to promote accountability. However, this tactic is a basic premise for understanding resistance in the era of big data: control of personal information is intimately related to democratic guarantees for the autonomous participation of citizens both in their traditional forms and in cyberspace modes:

> Snowden's documentation confirms that uncertainties about how we should understand democracy given the dynamics that are reshaping relations among states, and between states and civil societies, are rapidly merging with uncertainties about how we ought to be locating the political orders being structured in relation to new networks of intelligence and security agencies (Bauman, et al., 2014, pp. 135-136).

In Brazil, we also mentioned the case *VazaJato* as a paradigmatic example on this issue, in which independent media published leaks revealing the collusion of judges and attorneys to prosecute politicians. It is not possible to think in filling the gaps of accountability, like holding governmental agencies accountable before the public interest, without the struggles of those who disclose dire activities conducted in the shadows of organizations. A comprehension of the social, political, and economic dimensions related to accountability must be oxygenated with alternative strategies that expand the public sphere beyond legal rules and institutional boundaries. Tactics of necessary conflict are alternative paths that can legitimate policies or promote awareness, sometimes relocating informational power in favor of data subjects.

A final tactic based on confront is boycott. This classic tactic has being used from social movement to de-colonial groups during history. In the domain of digital struggles, one recent example is social media activism aiming to persuade companies to remove advertisements from specific news outlets. As disinformation, fake news, and counterpropaganda turn ubiquitous, some organization have specialized to counteract those strategies by cutting the financial supplies of media platforms. For instance, Sleeping Giants is a journalistic, activist, and anonymous campaign that started with a Twitter account to boycott Breitbart News, a far-right disinformation website. Suddenly, the campaign addressed advertisers who in turn stopped to associate their image and funds to controversial news, inflammatory rhetoric, polemic remarks and hate speech. By mixing strategies from the ironic and agonistic stream, this trend is now present in many countries, including Spain and Brazil. For instance, Sleeping Giants Brazil has acted against *Jornal da Cidade On-line*, *Conexão Política*, and *Brasil Sem Medo,* far-right and fake news outlets.

5.3.d. Despair stream

The despair stream relates anomy/altruism to conflict. That means, the use of tactics that intensify confrontation, including protests and riots. In this stream, individuals and groups might feel that the level of absurdity is as higher as the exceptional characteristics of politics. Here, there is less room to respond by the previous streams, either because those are not sufficient to challenge watchers or other hegemonic players, or because the other streams were blocked. In that context, a multitude of groups can promote deeper conflict to engage against the order. This case is similar to the suicide studies of Emily Durkheim, in which suicide can be committed by anomy isolation and circumstances that fragment the individual, or because the individual sacrifices herself for a greater cause to "save" the social cohesion (the nation, the people, the group, etc). In the same sense, severe conflict can arise due to the anomy fostered by instrumentarian surveillance that detaches individuals from communities, the fragmentation of social bonds, and precarious situations of living (in terms of material conditions, non-material expectations, and the horizon to accomplish them). In addition, the individuals and groups can feel they need to act themselves to the collectivity, by promoting radical attempts of change. Here the point consists of defining to what extent the radical conflict could be understood as legitimate. One should be careful to avoid quickly associations between these means of contestation with legal/illegal, good/evil, and other binary divisions.

At the individual level, one example happened in 2010 when Aaron Swartz created a script using the free programming language Python for downloading and distributing academic articles hosted on JSTOR, a digital library. In *Guerilla Open Access Manifesto*, he called for civil disobedience for the collectivization of world knowledge. Swartz was arrested and prosecuted for electronic fraud, computer fraud and illegally obtaining information by downloading JSTOR copyright-protected articles from MIT. Following his suicide, the United States federal prosecutors dropped all charges against the activist, which could have resulted in up to 35 years in prison and millions of dollars in fines (Da Silveira, 2013, p. 12). This case can be considered as both the combination of deliberative ideas (free access to information) with a deeper commitment to challenge the sociopolitical order that ended in his suicide.

At the collective level, as tactics of this stream, one can mention riots, unrest, massive protest, and even the use of violence in the digital infrastructure and the offline world. The collective action can be sparkled by the individual agency, as a result of many variables and dimensions that this study would not address. However, the tactics are specially produced in moments of dissatisfaction, and during key situations of effervescence and turmoil. In these cases, even violence can be committed but these events should be carefully read by the elements

affected (properties, life, immaterial values), the purposes (concrete claims, diffuse orientation), timing (progressive or eruption), and special scale (from local regions to the international level). Moreover, violence as a legitimate means was used especially in the 1960s and 1970s in our study cases. In the vision of violent groups, these actions were understood as attempts of self-defense to survive the subjugation of the centralized surveillance and to end authoritarian order. It does not mean that violence was legitimate or justified, let alone if these were effective to achieve their goals. Nowadays, because of the macro-political context (we will return to this in Part 4), violence seems to be frozen as an illegitimate tactic to be incorporated into resistance, especially when it takes other's life. In this sense, the equation is very simple: if the source of legitimacy stems from the people, subtracting the chance and opportunity to agglutinate more voices to construct legitimacy implies in suppressing the very elements of legitimation. Murder, for instance, is not only morally unjustifiable but also suppresses the sources of legitimacy through utilitarian methods and dehumanizes any political clash. In part, groups like the Basque ETA lost internal support and made a shift in the last decades to abandon violent tactics as a way to promote political change (Murua, 2017). All the same, the use of violence to seek legitimacy and promote resistance is a sensitive point and its incurrence could entail the problem of "disgusting politics" that we addressed in Chapter 1. A logic in which beautiful endings cannot be reached by abject means. Paradoxically, beautiful politics, without its counterpart, is limited to promote social transformations. In that sense, beautiful and disgusting politics was conceived as a dialogic relationship that produces a dynamic tension (rather than a binary division to formulate static assumptions or easy categories to label complex social phenomena).

As examples of tactics in this stream, some paradigmatic cases happened in the recent decade. From phenomena such as the Arab Spring, the Spanish 15-M, the Occupy movement, the Icelandic revolution, the Brazilian marches, the Lebanese revolts, the Hong Kong protests, the Chilean uprising, and so on, all of them brought substantial changes in dialectical dynamics of confrontation and conflict from multitudes that were not conformed to their social realities. They confirmed the rise of new forms of networked political action. It is not always clear what ideas, experiences, tactics, or projects hide behind such actions. However, in a general view, it can be said that those movements influenced each other. Furthermore, they refer to a set of technologies and practices that point to a reconstruction of political action and public space.

For example, when the images and news of a massive revolt arrived in Tunisia against the Ben Ali regime, Egypt and other Arab countries entered in turmoil in 2010. In this year, Wikileaks released cables that reflected the extent to which the Tunisian regime was corrupt. But this was not enough to rise the protests in this country. In fact, the chain of events was triggered after the self-immolation of Mohamed Buazizi on December 17, 2010. Buazizi was a young street vendor who

was extorted and humiliated by the police when they seized his fruit stand. In protest and despair, he went to the town hall in Sidi Bouzid to burn himself. Hours later, friends and other vendors uploaded the immolation scene to the Internet and protests started against the government. The outrage circulated in a social environment marked by dissatisfaction, high costs for living, and disenchantment of millions of Tunisians. Buazizi died on January 3. In the meantime, the protests had spread throughout all Tunisian cities. Government repression increased the turmoil and the protests, in turn, spread to more countries. Despite the authoritarian backlash effect in many Arabic countries in recent years, the Tunisian experience served as an example for other mobilizations, such as the Tahrir Square tactics used in Egypt and the Madrid occupy movement (15-M) in 2011.

The 15-M movement was also inspired in the dissatisfaction echoed on March 2004 when thousands of people surrounded the headquarters of the Popular Party (PP) to protest against the Al-Qaeda bombings in a train station two days before in Madrid. At the time, the Popular Party government gave unclear accounts and contradictory information about the authorship of the attacks. People then organized themselves through text messages (SMS) to protest. Those actions glimpsed the power of connected multitudes years later on May 15h of 2011 (15-M). In the latter event, these tactics were even taken further, consolidating the self-creation of a "distributed movement of collective bodies using social networks to overtake public spaces in the whole country" (Toret J. , 2012, p. 63). The economic crisis and the worsening living conditions of a large part of the population, especially young unemployment rates that reached nearly 50%, plus the intense crisis of representation of the institutions, were ingredients that facilitated the collective revolt and fostered more social and political participation. In short, in the eyes of the protesters, the Spanish sociopolitical order was dying and needed deeper changes. The 15-M gathered 12 million people and convoked riots in 70 cities, something totally new since the Spanish transition initiated in 1975.[139]

As a result, in January 2013, Party X was created advocating a model of participatory democracy, exploring the political potential of digital communication tools. Its program was based in the citizen legislative power (wiki democracy); and the application of binding referendums. While this party did not consolidate itself in the Spanish political system, Podemos had a different destination. Founded in

[139] "In order to force the system to an unsustainable position, you cannot demand the opposite side to "destroy itself" because it will prepare defenses and consider you as the antagonist. However, if you force a closed system of privileges to "improve" itself, it will show its contradictions and implode, but this implosion should be reached as an exit way, there must be an escape route to the system. We all know that the enemy must have a way out if we want to win. And we must also learn to win because the accusation that harms us the most, since it causes to lose communication with a large part of the people, is not that we are some violent, but that we are just a bunch of kids protesting, with no offers or proposition to govern and this is not truth" (Alcazan, Axebra, Levi, SuNotissima, & Toret, 2012, p. 44).

February 2014, the left-wing party, alongside Ciudadanos, the new liberal right-wing party, redefined the landscape of political elections since that year. We have no intention to analyze their trajectories, but there is no doubt that the Spanish procedural democracy has entered into a cycle of reformulation since 2014, as well as the return of substantive nationalist challenges, from "peripheral" communities as in the case Catalonia, and the rise of centralist and conservative forces as in the case of *Vox* far-right party.

In Brazil, the Confederations Cup riots, also known as the Vinegar Movement or Brazilian Spring of 2013, were initiated by the *Movimento Passe Livre* (Free Fare Movement), a local entity that advocates for free public transportation. The manifestations were initially organized to protest against the rise of bus, train, and metro tickets. Suddenly, the movement included other issues such as the high corruption in the government and police brutality used against protesters. By mid-June, the movement had grown to become Brazil's largest manifestations since the 1992 protests against the former president Fernando Collor de Mello. In that time, frustration growth among the general population due to the inadequate provision of social services and the overspending in mega sports events. Despite Brazil's international recognition in lifting 40 million people out of poverty (Awan, 2014), there was no synchrony between the expectations of many Brazilians and the actualization of economic and social opportunities. It is not saying that all protests were caused by despair, by this logic permeated and agglutinated even more people that reacted and mobilized. "We left Facebook", was the slogan of many young people as they transferred their critiques from the Web to the streets. The interconnected-multitude aimed at short-term objectives such as freezing the transportation fares and repassing petroleum royalties to education policies. Also, structural demands such as a political reform via referendum were added to the agenda in the ongoing process although these demands failed (Saad-Filho, 2013).

In 2016, after the economic crisis and Dilma's re-election by a slight difference (51% of the votes in a majority system), a new cycle of protests against her administration took place in Brazil. The movement was triggered by the perception of corruption involving the state-sponsored oil company Petrobras and by the repercussion of white-collar investigations of the Lava Jato operation involving the government. At the climax of this process, a broad spectrum of society was mobilized by different claims that coexisted in the same physical space despite the different ideologies and expectations.[140] However, Tatagiba & Galvão (2019) mention that, in the protests cycle from 2011 to 2016, the internal economic crisis and the slow social mobility evidenced the limits of the Workers Party (PT) to govern the country. Thus, those years were marked by the emergence of new forces on the left and especially on the right. The latter

[140] Bringel, B., 2016, February 18. '2013-2016: polarização e protestos no Brasil'. *Open Democracy*. Retrieved from https://www.opendemocracy.net/pt/democraciaabierta-pt/2013-2016-polariza-o-e-protestos-e-no-brasil/ in 02/13/2020.

increased its visibility on the streets, fostering anti-establishment ideas linked with conservatism ideologies. Groups such as Free Brazil Movement (MBL), which supports free-market responses to the country's problems, and Revoltados Online, supporting patriotic and anti-communist ideals, rescued the Cold War polarization and shared daily anti-government publications on social media and helped to impeach Roussef in 2016. Those groups also gathered millions of followers and paved the road to the campaign of the iconic Congress member Jair Bolsonaro, who was elected as the Napoleonic solution to "solve" the problems of the country in 2019.

The despair stream is a breeding ground for experimentation and redefinition of politics that congregates the multitudes in key moments of history. The outcomes are various in the short and long terms. As the history of both countries is still being constructed, in short terms, the outcomes of the multitude were channelized to a scenario of polarization and fragmentation in the Spanish polity (institutional) system, and in a conservative and ultra-nationalist program in Brazil. This not means that multitudes or their civic actions were inevitably oriented to those ends. The variables behind those collective actions are many and any causal explanation to those new situations escape to our objective. Notwithstanding, either by deliberative, agonistic, and despair notions to reconstruct social interactions, it is impossible to point out the ultimate direction to the civic agency. Spanish activists like Javier Toret expresses that the lack of this ultimate orientation is one strength of the multitude, rather than a weakness point. In his words,

> The massive appropriation of private and corporate social networks and the invention of new free tools, added with large-scale hacktivist strategies for the sake of organization and political-viral communication, have opened a new field of socio-technical experimentation. This is the scope of what we call "Technopolitics". Technopolitics is a collective capacity for the appropriation of digital tools for collective action. […] The best thing about the network is the absence of Generals, the power of the connected multitudes resides precisely in their networked and distributed character. This is real power and must be defended (Toret J. , 2012, pp. 7, 13).

In his defense the decentralized power of the connected-multitude, Toret even supports the appropriation of traditional electronic tools and the encounter of deliberative and agonistic streams. For example, Facebook and Twitter played a key role in the emergence and development of the 15-M (Indignados) movement. The possibility of forming groups on Facebook made it more suitable for the collective organization. This was the case of coordination platforms such as Democracia Real Ya (Real Democracy Now). Twitter, on the other hand, was characterized by short-lived messages transmitted instantaneously for many people. Hence, those were ideal tools for mobilization and transmission of

immediate information in the context of street mobilizations. In Brazil, those possibilities were also explored in the marches that took place in June 2013. The demonstrations against the rise of bus tickets started in the city of Porto Alegre, and soon all 27 Brazilian states organized more protests. By content produced directly from the streets and disseminated in real-time through social networks such as Twitter and Facebook (organized through hashtags #vemprarua and #ogiganteacordou), Brazilians expressed themselves in huge proportions that challenged even the traditional media.

However, new communication networks (media 2.0) have not replaced the traditional media in those countries. The techno-politics of the multitudes has not the same capacity to shape or perform cultural cognitive frameworks to the same extent as the traditional media and the mass culture industry. Yet, the connected multitudes can influence the content of the large media through viral network campaigns that, by force, they end up echoing by hybridisms (Gulyás, 2016). Here, deterministic visions to formulate the best strategies to be adopted by the multitude might be elusive because of the heterogeneous and constant changes in this domain. Rather than a simple view of hierarchical terms between media 1.0 and 2.0, what is clear is the increasing overlapping interdependence between traditional media and the multitude to produce information. In that project, civic strategies and resistance are an array of attempts to construct new realities –even if these attempts are a provisional set of informal practices- bargaining power against hegemonic political forces. In that sense, accountability promoted by civic agency strategies can be edited to mitigate "the regression of democracy into hierarchical forms such as bureaucracy or oligarchy, which in turn may offer a mask for inefficiency and corruption" (Warren in Malcolm, 2008, pp. 260). Unfortunately, this trend is being suppressed in the current development of historical facts in both countries, especially in Brazil.

In the meantime, the demand for better accountability projects sparked by the civic agency has reached even the international level. As the global economy shifts further into a connected information space, the relevance of data protection and the need for controlling privacy will further increase. The 2016 United Nations (UN) "Conference on Trade and Developments" recognized the importance of data protection regulations and international data flows for commercial and civil purposes. The UN encouraged actual collaboration amongst multi-stakeholders and non-institutional partners to expand the communicative scope of interaction on the Web. Besides, The UN claimed to balance surveillance and data protection, especially after national security and mass surveillance revelations since the Snowden case in 2013. This claim is important but data protection empowering data subjects cannot automatically guarantee more participation and democracy on the Web. Elena Pavan's explorations of online activism, for instance, demonstrated a high degree of fragmentation in communication patterns. For Pavan, active exchanges of opinions and virtual forums might merely play an

informative role in the majority of occurrences. “Compared to other international issues like global justice and peace, environmental concerns, etc., Internet Governance demands greater communicative and mobilization capacity to raise more attention among audiences” (Pavan, 2012, p. 112). Yet, as we show in this section, civic agency strategies can go beyond the mere informative roles or deliberative scope, and work in agonistic and despair streams. This becomes even more relevant as every issue, from political elections to social unrest, is being affected by the interconnected-multitude who exercises pressure and is pushed by other players from state-forms and markets. In this “triangle” of power relations, accountability is not taken for granted but it might be constantly reformulated to replenish the power asymmetry between personal data subjects and data processors.

Epilogue

So far, the impact of civic agency tactics to enhance accountability is still debatable. In other words, the streams shown above require a deep level of awareness of surveillance representation, technologies, and meanings to calibrate the tactics and responses of the citizenry. Many critiques could arise because of the array of responses and lack of a common orientation to resistance. Yet, as attested in the discussion, the civic multitude must be understood in plural terms and especially by the mutable modulation of relations of power. That is, in the same logic that surveillance is a modulation of control, resistance has many fronts, many purposes, and even contradictory logic. Resistance is not the essentialist or absolute battle against someone/something. The strategies of the multitude are mutable as the collective actions hinge on the flexible adaptation of tactics and goals. The attempt to bring a new reality, awaken by the non-conformation to “normal” standards and dispositives of surveillance, keeps resistance moving, allows the multitude to be heterogeneous, and, necessary to say, makes surveillance evolve to reestablish control upon the watched. In the last decades of the twentieth century, resistance was understood as a game between “mice and cat”, a chess game to overthrow the king of the board, especially by the despair stream during the 1960s and 1970s in our case studies. After the rise of informational and digital societies, today the most similar allegory would be the interaction between different species and niches in ecologic systems, or the non-linear “Go” game, in which pieces dispute spaces and movements to surround the adversary in the strategic board. Rather than a match to capture the king, we have entered in a game of continuous disputes and movements.

However, indeed we can think in two different levels to agglutinate the above streams of resistance (ironic, deliberative, agonistic, and despair). That is,

there can be two broader levels in which resistance streams operate: at the **agency level**, and the **meta-agency or structural** level.

In surveillance, the near-agency level consists of understanding resistance as the relational principle between the watchers and the watched. Here the gaze is important to mediate and constitute power between actors. The tactics in this level consist of trying to identify the watchers, the technologies of surveillance, and the dispositives used upon the watched. It consists of looking at resistance as a goal that oscillates between its internal principles and the attempt to explore the niches, circumstances, and opportunities to challenge surveillance. In simple terms, this is the level in which tactics are addressed against surveillance by direct means (communicative, cooperative, confrontational, and conflictive).

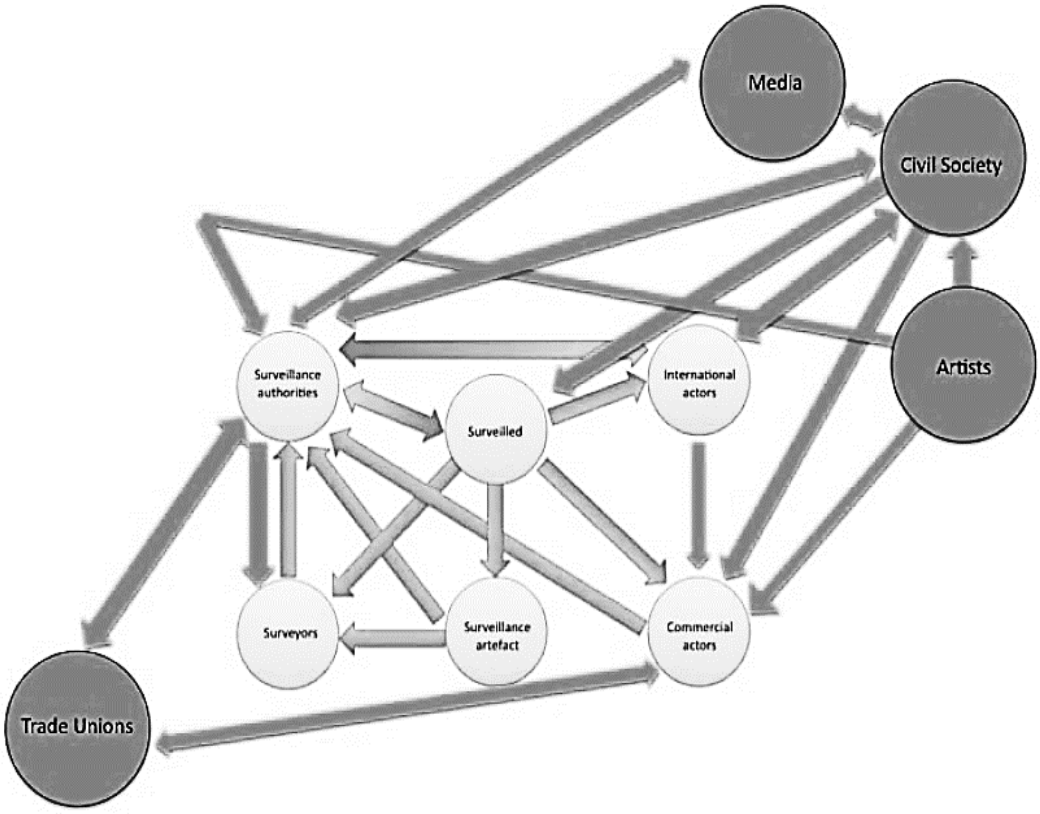
On the other hand, the meta-agency level consists of looking beyond the initial actors and tight conditions that promote and involve tactics of resistance. It goes beyond the relationship between specific watchers and watched, or between specific players at stake. At this latter level, resistance aims to tackle non-identified gazes and the structural conditions that allow or produce the gazes. In other words, this is the level in which surveillance is just one part of a broader game; a piece in the structural puzzle in which resistance is taken to non-foreseen consequences and goals. It is similar to the fog of war that permeates resistance actions to non-recognizable practices and orientations. These unknown directions, whether in terms of undefined players and gazes or uncertain strategies and outcomes, would be very important to agglutinate the different streams of the agency to ulterior levels of change in the social structure. We will return to this point in Part 4 of this study.

The near-agency or agency level can be identified with the molecular level, that is, the micro and meso domains where resistance can be promoted especially to tackle surveyors and challenge their direct power, without major changes in the structure or the sociopolitical order in a broader sense. Here, ironic and deliberative tactics can help to deconstruct and agglutinate changes that alter the surveillance assemblage in specific places and rhizomes. In turn, the meta-agency or structural level corresponds with the molar level, the macrosocial scale in which resistance tactics can be created to overturn the logic between "watchers and watched", altering the performance of rhizomes in the surveillant assemblage and beyond.

To put in context, the difference between the agency level and the meta-agency level can be appreciated in the generic diagram of Figure 19. Martin, Van Brakel & Bernhard (2009), in a study of the United Kingdom National Identity Scheme, already explained the necessity of proposing studies and models of resistance through multi-disciplinary and multi-actor frameworks. They identified that the concept of resistance remained underdeveloped and focused on relations

between the surveyor and the surveilled, neglecting other relevant actors. To expand the list of relevant actors, they propose a map of complex resistance relationships beyond the watchers and the watched. In our understanding, those authors were looking for relations beyond the agency level. Beyond surveillance authorities, commercial enterprises, international governmental and non-governmental agencies directly related to the implementation of the National Identity Scheme. By expanding those relations to actors beyond the direct issue of surveillance, but still affected by this domain, they were able to look into elements of the structural or meta-agency level. This comprehension attested the necessity of understanding multi-actor resistance relationships at various stages of the scheme's development. In this concrete case, the lighter nodes in the figure below refer to those actors within the agency level: surveillance authorities, surveilled, surveyed, surveillance artifacts, etc. Meanwhile, the external darker nodes can be associated with general actors that bring more context beyond surveillance, such as trade unions, civil society, the media, and artists. In that sense, the whole diagram of nodes and relationships would represent with a cluster in the meta-agency or structural level.

Figure 19: Expanding the surveillance framework (to the meta-agency level).



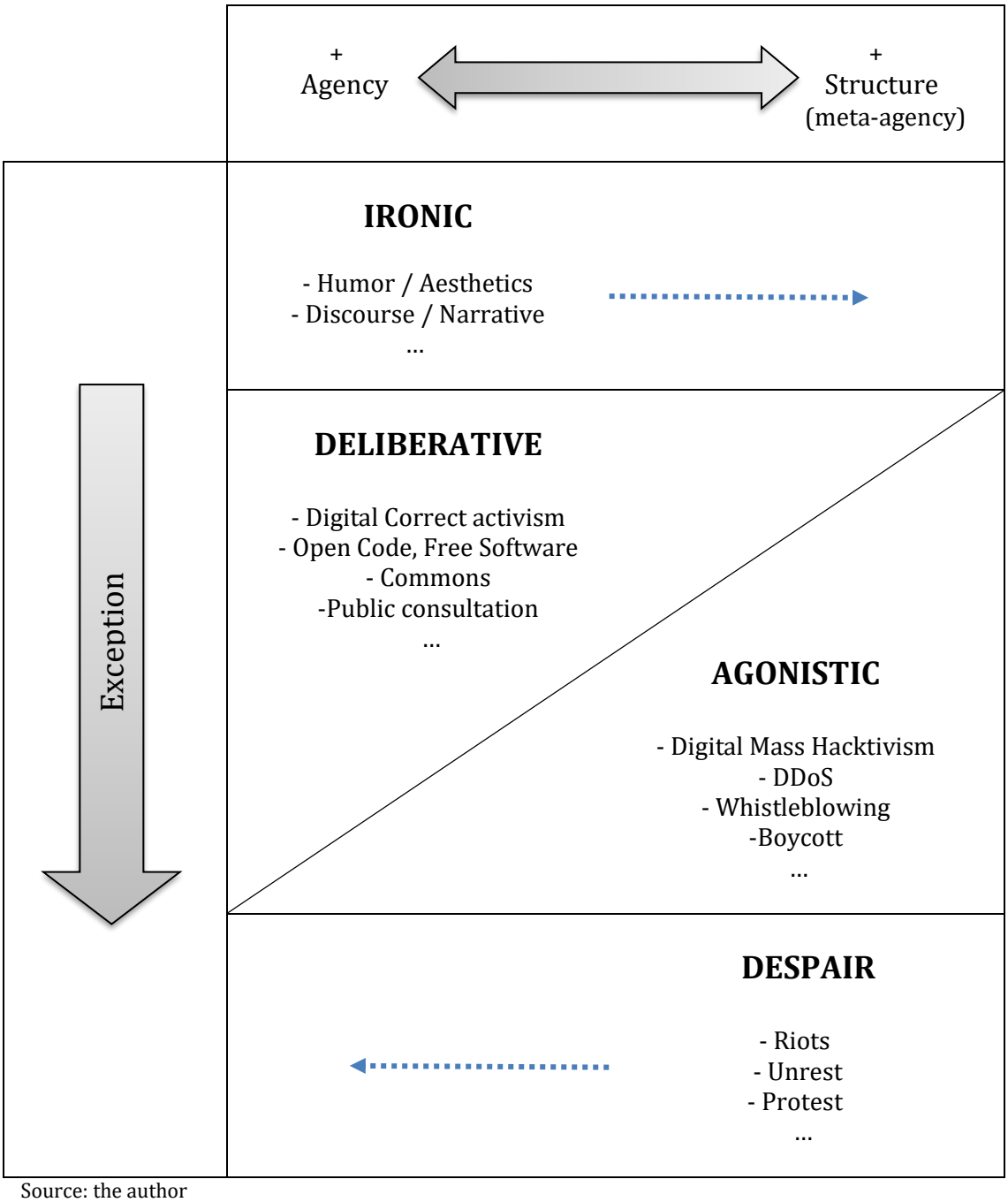
Source: (Martin, Van Brakel, & Bernhard, 2009, p. 228).

When it comes to studies in resistance, Dencik, Hintz & Cable (2016) also claimed the necessity of going beyond issues directly related to surveillance. For

them, resistance to surveillance in the wake of the Snowden leaks has predominantly centered on techno-legal responses relating to the development and use of encryption and policy advocacy around privacy and data protection. For Dencik et al., there was a level of ambiguity around this kind of anti-surveillance resistance in relation to broader activist practices, and critical responses to the Snowden leaks have been confined within particular expert communities. Hence, they introduced the notion of 'data justice' as resistance to surveillance needed to be (re)conceptualized in relation to broader social justice agendas. Such an approach is needed, they suggested, in light of a shift to market surveillance in which the collection, use, and analysis of data increasingly comes to shape the opportunities and possibilities available to citizens. In our vision, data justice was another answer in the direction of connecting resistance to the meta-agency level. That is, incorporating broader social justice agendas in surveillance implies adding structural components in the analysis of resistance.

Naturally, changes in the meta-agency level are more difficult and require greater logics of contestation. In our view, the agonistic and despair streams tactics are examples in which the multitudes seek to promote changes beyond the agency level. In the unrest and mobilization of Spain since 2011 and Brazil since 2013, many people did not know who decided, who watched and even ignored the concepts of power entailed by surveillance gazes. That is, in many events surveillance is not directly challenged by people. Yet, surveillance can be contested by indirect means. Almost nobody went to protest in the streets against the algorithms of Facebook, or few people promoted strikes for better data protection rules. However, when the multitude went to the streets, they coalesced tactics to challenge surveillance by diffuse grievances that are transversal to surveillance, like social justice, transparent governments, and dignity to live. In these situations, people are not necessarily indifferent to surveillance as they demand structural changes that also affect this realm. Thus, the general and diffuse grievances that not mention surveillance at the structural level are as important as direct causes against surveillance at the agency level. Considering this complementary nature and holistic perspective about resistance, we summarize the tactics, streams, and levels of resistance in the following table.

Table 19. Resistance in a comprehensive framework



Source: the author

The table shows the streams of resistance that we proposed in this section. Each stream contains a list of specific tactics of action. For example, the ironic stream comprises especially those tactics focused on the communicative action, such as humor and aesthetics, discourse, and narratives. The logic of the Deliberative stream is cooperation. As deliberative tactics, we mentioned Digital correct activism, open codes, commons, and public consultation. The logic of the Agonistic stream is confrontation, as in the case of Digital Mass Hacktivism, DoS

(Denial of Services), whistleblowing, and boycott. Lastly, the logic of the Despair stream is conflict, exemplified by riots, unrest, and protests.

The above tactics are just some important examples. Thus, the list of tactics in each stream can be expanded and changed as the multitude re-appropriates or incorporates more resistance actions. There is no hierarchy between the streams in our model. Furthermore, the streams can be combined and are interdependent from each other to promote social transformations. However, there are two patterns among the streams that are represented on the left and superior sides of the table.

The left side indicates that there is a growing perception of exceptionality in the tactics and streams. As we move downwards, there is an increase in the scale of exceptionality: the level of uneasiness and political leeway that sustain the non-conformity with "normal" situations in order to challenge surveillance and surveyors and generate "new" politics. In short, exceptionality level indicates resistance in terms of abnormal reactions and generation of changes. The level of exceptionality increases as we move to despair tactics, in which, as attested in the previous pages, the non-conformity with governmentality dispositives was replaced with direct conflict and the open challenge of the sociopolitical order to generate new political scenarios.

The superior side of the table indicates that resistance streams operate or specialize in two social levels: agency and structure. The ironic and deliberative streams tend to specialize but are not limited to the agency level (actors level), whereas the agonistic and despair streams tend to specialize but are not limited to the structural level (meta-agency or macro-political context). For example, in the ironic stream, language entails resistance especially in agency levels as no regime was overthrown just by the use of jokes or communicative actions like propaganda, especially when they committed violence and created overwhelming situations of oppression. Nonetheless, the ironic tactics served to complement and even create new tactics in other streams. It does not exclude that even the ironic level and the use of language can have impacts on the structural level. We know that language help to re-think the structure. In that sense, the Canadian writer Daphne Marlatt and many other feminist writers reflect and challenge the relation between autobiographical paradigms, geographical metaphors, and social authority. Marlatt rejects the "explorer" metaphor that establishes man-in-place, man-with-the-power-to-chart-and-name. She rejects the male intellectualism of map-making asking "who has the right to speak? Who has language available to them? Who is privileged by existing linguistic conventions? (who is not made marginal?)" (Marlat in New, 2003, p. 248). Those questions not only rethink language itself but open lines to demand more changes in the social structure. Thus, ironic and deliberative streams can be produced at the agency level and

extended to structural levels as indicated by the superior dotted arrow in the Table.

On the other hand, the greater the scale of exceptionality, the more the streams of resistance tend to focus on the meta-agency/structural level. Riots and unrest tactics can affect the reconfiguration of the structural level in a broader sense because of the mass conflict promoted. Despite this capacity, they depend on the agency, on concrete actors, and on other streams to fulfill and congregate multitudes. Thus, contrary to ironic and deliberative, agonistic and especially despair streams should expand their logics in order to re-connect with agency actors (inferior dotted arrow in the Figure). Besides, a despair tactic with no complementary ironic and deliberative tactics might lack support to reach deeper social transformations in the structure, no matter the scale of exceptionality that is present in the environment. In part, lack of that support explains why many conflictive tactics fail to implement changes in the structural polity. For example, the focus on violent actions disconnected the separatist group ETA from the first streams in the Basque society, explaining part of the failure to alter the polity and the governance structure in this region since the 1980s (Murua, 2017). In Brazil, during the mass protests in 2013, the despair tactics from the multitude produced a gap that was not filled by deliberative and agonistic tactics to promote political and electoral reform. Years later, in 2016, the plurality of the multitude decreased and the gap was filled by ultra-nationalist and conservative actors that reinforced the authority of the establishment and blocked the reform of polity institutions.

Thus, instead of isolated streams, the model shows an ecological sense of interdependence. In real practice, those streams appear combined or intertwined with other ones in different moments of history. In an overall sense, all the streams are sustained and obtain inputs from the ironic or communicative stream. Yet, different experiences and contexts would emphasize certain streams rather than other ones. However, when the four streams emerge maximized in parallel (not only in sequence), the conditions for a "perfect storm" of resistance are created. In this case, the streams can support each other in terms of temporality (they last longer), or in terms of intensity (they erupt on a greater scale of mobilization). In the "perfect" situation for resistance, all the streams contribute to reinforce each other and achieve structural transformations. Those situations would correspond with revolts, rebellions, and even the start of revolutions.[141]

Exploring the key political elements, the conditions and the specific moments when those ideal situations interplay to create greater levels of structural change escapes from our objective. Yet, agency strategies as well as

[141] Even in the case of revolution, the interdependency of different tactics and groups is a basic notion to this kind of events. For Tilly et al. "for participants or their successors to decide that an episode qualifies as a revolution or as a huge riot makes a difference to the identities activated, allies gained or lost, governmental measures the episode triggers, and readiness of other citizens to commit themselves in the course of later political action" (McAdam, Tarrow, & Tilly, 2003, p. 228).

structural calculations are not outside of the mechanisms of transgressive contention but are the raw material for their action and interaction (McAdam, Tarrow, & Tilly, 2003, p. 226). This became clear as the Spanish and Brazilian revolts in 2011 and 2013, respectively, fostered deep alterations in the political structure that started in 1978 in Spain (after the Franco regime) and 1988 in Brazil, since the proclamation of the Constitution.

In short, the interdependence between the streams and their position in the agency/structural level also indicate that ironic and deliberative tactics need to create "equivalences" and produce broad meanings; empty signifiers, to use terms of Laclau (2008), in order to reach more audiences and structural levels. Meanwhile, despair and agonistic tactics would need to granulate their content in order to reach agency or concrete actors by capillarity, as indicated by the arrows in the last Figure.

In the case of the Spanish and Brazilian revolts, the sociologist Manuel Castells claimed the interdependence between different tactics emphasizing the deliberative approach.

> They [the multitude agency] generate their own forms of time. The movements live the moment of the occupied places and, at the same time, the horizon of the continuous processes and the projection of the future. The movements are spontaneous in origin, usually triggered by a spark of indignation. Then, the movements are viral: they follow the logic of internet networks. And, sometimes, the transition from indignation to hope takes place through the deliberation of the space of autonomy: a self-governing movement by the participants. Horizontal networks create fellowship and a sense of belonging (Castells, 2013, p. 160).

The overlapping characteristics of the streams can also be verified in agonistic approaches, as expressed by the activists Toret & Pérez de Lama (2012) in their analysis of the same event:

> The revolution is not only played in the field of manifest political discourse, but also on a much more molecular level, which concerns the mutations of desire and the technical-scientific, artistic mutations, etc. These are the wishes and knowledge of the active connected multitudes who invent tactics and strategies of construction for empowerment and social and cognitive mobilization. Those are struggle-invention tactics (Toret & Pérez de Lama, 2012, p. 28).

Discursive tactics evolving to reinforce conflictive actions in mass resistance is a regular characteristic of the multitude. For example, the sharing of communicative actions reinforced despair tactics across the world in the last decade addressing the special issue of political representation.

> 'They Can't Represent Us!' was a slogan heard ringing through the streets of Russia during the democracy movement of 2012, alongside 'They Can't Even Imagine Us!' In Cairo's Tahrir Square, it was Kefaya! ('Enough!'); in Athens's Syntagma Square, banners declared, in Spanish, ¡Ya Basta! ('Enough is Enough!'); in Spain, the banner ¡Democracia Real Ya! was a unifying call. Each country had its own variation on this theme – 'We've Had Enough! We Are Fed Up!' in Turkey; Eles Não Nos Representam! in Brazil; 'Screw the Troika, the People Must Rule'! in Portugal. Perhaps the one English readers will know best is 'We Are the 99 Percent!' – the Occupy movement's slogan throughout the United States (Siltrin and Azzelini in Burgos, 2016, p. 20).

The lack of connection between authority and legitimacy was evident in slogans and protests across the world, including our cases. In that sense, massive resistance interprets political representation as a distorted and disconnected issue from the multitude. This alleged misrepresentation or illegitimacy, then, would need to be recalibrated especially in moments when many tactics from the streams converge.

On the other hand, for traditional watchers, and hegemonic players at the structural level, the "perfect" situation for resistance would correspond with the "perfect storm". Their objective would be to avoid greater levels of intolerable exceptionality and the conjugation of the different streams. Yet, as those elements are not fully controllable, multitudes marching against their interests appear in specific moments in history. However, it does not mean that surveyors do not "watch" the tactics and the logic of resistance in each stream. Counter-narratives and disinformation tactics have been used by the diplomacy of states and by big companies throughout history to counteract adversaries or protect their strategic position (Bjola & Pamment, 2018). In that sense, the ironic stream is a crucial battlefield as inaccurate information or dubious narratives can produce the effect of "disorientation" and "delegitimization" of sources of information. In part, those tactics were applied by new parties and advocacy groups who patented the combination straight talk + attacks to the mainstream media + unchecked social media messaging.[142]

Either by the heterogeneous voices from the multitude or by counter-resistance narratives, disorientation can create the conditions to reinforce conservatism appealing to the psychological archetype of authority as a corrective figure based on fear and anger. In psychological terms, persons whose power or lack of power is exclusively based on imposition and manipulation might suffer from powerless or authoritarian scripts that reinforce each other (Steiner, 1987).

[142] Dilorenzo, S.; Pregaman, P. 2019, December 14. 'How Brazil's Jair Bolsonaro used Trump tactics to move to 2nd round of presidential race'. *USA Today*, retrieved from https://eu.usatoday.com/story/news/world/2018/10/08/brazils-jair-bolsonaro-used-donald-trump-tactics-presidential-race/1565689002/ in 02/15/2020.

Indeed, general people as well as official authorities and security actors might fall into that archetype. Thus, the problem is not appealing to traditions and authority, but to use it to distort information or promote a messianic logic marked by an idealized past and dichotomies between "we the good people" against "them the evil" (Hameleers & Schmuck, 2017). This kind of warfare has been taken to the civil sphere of digital communication to create a myth of authority based on strong leaders and messianic saviors, as in the case of the recent political campaigns in Brazil and Spain.[143] People have legitimacy to claim for order, discipline, and a peaceful life. But the same claims are controversial to promote counter-resistance scripts that erase pluralism and mistake cooperation and generosity with inferiority, or force and cruelty with a superior nature. Moreover, a leader can appeal to the multitude and be popular, but he/she cannot concentrate all the authority and legitimacy stemmed from society. As explained in Chapter 1, those poles are not concentrated in one person or organization. Thus, authority and legitimacy must be recalibrated all the time.

In terms of counter-resistance, watchers can direct their efforts beyond the ironic stream to avoid the ideal conjugation of resistance or the "perfect storm". For instance, in the deliberative and agonistic streams, a report by the Spanish National Intelligence Center (CNI) emphasized the decline of hacktivist tactics in the country from 2010 to 2020. The report mentioned that "The hacktivist reality is characterized by individual profiles of null or low technical expertise (conducting cyber threats), and by weak groups with no identity". Hacktivism, according to the report, is on the way of becoming "cyber-graffiti" or "cyber-exhibitionism" from an "anti-system and anarchist ideological base".[144] If the report is correct, hacktivism might decay as the anarchist tactics that challenged states in the first two decades of the twentieth century. Yet, past events can be similar but history never repeats itself. Also, deliberative and agonistic streams can reformulate their tactics as they face counter-resistance and surveillance, as exemplified by the sample of actors in Table 20. The decline of one tactic certainly undermines the civic agency but not necessarily causes its permanent decline.

---

[143] Alessi, G. 2018, October 29. 'Contradições e bate-cabeça da campanha de Bolsonaro são intencionais'. El País. Eleiçoes 2018. From https://brasil.elpais.com/brasil/2018/10/24/politica/1540408647_371089.html, consulted in 02/15/2020; Castillo, C. 2019, October 31. 'La trama a favor del PP en Facebook se hacía pasar por simpatizantes de otros partidos para desmovilizar a su electorado'. *El Diario*, tecnología. From https://www.eldiario.es/tecnologia/PP-Facebook-simpatizantes-desmovilizar-electorado_0_958554526.html, acessed in 02/16/2020.

[144] González, M. 2020, April 15. 'El servicio secreto sospecha que el independentismo usa a falsos hackers para difundir datos sensibles'. *El País*. Retrieved from https://elpais.com/espana/2020-04-14/el-servicio-secreto-sospecha-que-el-independentismo-usa-a-falsos-hackers-para-difundir-datos-sensibles.html in 02/17/2020.

Meanwhile, the despair stream, which is closely related to possible impacts on the structural level, is often the most suppressed and counteracted stream by hegemonic actors from different realms. Not only because this might be labeled as illegal, violent, and even chaotic by their antagonists, but also because it presents a conflictive nature that would demand strong responses. However, the suppression of this stream by violent means and disproportional answers can feed other streams of resistance that, in turn, challenge the establishment by other tactics, reinitiating the cycle. Here, counter-resistance can follow again the corrective script of authority. Indeed, a corrective authority overreacting to suppress the despair stream was also observed in the Spanish and Brazilian revolts analyzed above. In that sense, monitoring the stream that is closely related to the structural level would delay, and perhaps avoid, deeper changes in the social order.

Despite being monitored by the watchers, it is important to remind that the tactics and streams of resistance are not necessarily illegitimate, even if they are illegal. The sources of legitimacy stem from the multitude. Yet, even when those sources are distorted by illegitimate means like violence, this does not justify unaccountable answers for the sake of security or to normalize the social order. From humor narratives to riots, the assessment of the streams should be carefully conducted in a posteriori manner (after concrete actions and outcomes). Some cases like protests and dissidence are even ensured as constitutional rights and legitimate forms of contestation. Thus, one problem arises when surveyors and automated machines, in their preventive logic and a priori assessment of targets, interpret the resistance streams in a scale of radicalization that increases from the ironic to the despair stream. If groups from the multitude change their tactics from discourses to conflict, it does not mean they have become illegitimate, neither their actions should be suppressed a priori. Each of the motives, outcomes, and changes of tactics need to be taken into account in order to assess resistance clashes and formulate legitimate and proportional answers. Otherwise, counter-resistance might become illegitimate. In turn, this could enhance even more exceptional levels of contestation and new forms of resistance in the streams, restarting the cycle. Naturally, not every demand from the people is legitimate, especially if they appeal to disgusting means and authoritarian ends. However, when politicians become alienated elites instead of representatives, when security agencies become correctors of people instead of servers and mediators of them, and when companies turn into grids to commodify individuals rather than producers of social goods, the conditions to demand structural changes could be necessary by the imperfect array of demands, general grievances, and collective strains from the multitude.

To end this section, let us consider some samples to exemplify the streams of resistance. To do so, we have chosen nodal actors from the Spanish and Brazilian interconnected-multitude that have been agents of resistance in the last years. We considered the main characteristics described by the actors in their

websites, thus, the categorization is auto-referential. It is based on the self-representation that actors make of themselves in descriptive terms. In analytical terms, the representation can vary according to relations and dependence on other actors. The samples are random and extracted from bibliography and news articles during the last years in both countries. They don't indicate a political spectrum, personal preference, neither a representation in terms of volume in each stream. Rather, they elucidate the mosaic of actors in the interconnected-multitude, as well as their potential and fluidity to dialogue/challenge other actors according to their tactics of specialization.

Table 20. Sample of nodes and tactics of resistance.

Node: *Privacy International.* Privacy International is an independent charity and all our campaigns against companies and governments are driven solely by our aims: to promote the human right of privacy throughout the world. This is why we do not accept any funding from the industry. **Tactics:** Discursive/Narrative **Stream:** Ironic
Node: *Algorithm Watch.* AlgorithmWatch is a non-profit research and advocacy organization to evaluate and shed light on algorithmic decision-making processes that have social relevance, meaning they are used either to predict or prescribe human action or to make decisions automatically. **Tactics:** Discursive/Narrative + Commons **Major stream:** Deliberative
Node: *La Asociación Profesional Española de Privacidad.* A non-profit entity, a group of professionals dedicated to privacy and data protection of different areas, especially in these lines: legal, technical, academic, both public and private. We have the aim of providing professional expertise with special status and recognition in the sector. **Tactics:** Discursive/narrative **Stream:** Ironic
Node: *Red.es and the General Secretariat of Digital Administration (SGAD).* As part of the Ministry of Finance and Public Function (MINHAFP), the SGAD offers service to the Public Administrations through the Technology Transfer Center (CTT), in order to facilitate the creation of new reusable solutions. The reuse of software begins in the moment of the formulation of the applications and continues during its development, distribution and evaluation, in a continuous cycle. Among those tasks, the SGAD verifies the compatibility of open source licenses and associated components, selecting appropriate licenses and giving recommendations and technological solutions. **Tactics:** Open code **Stream:** Deliberative
Node: *El Campo de Cevada.* Digitally self-organized collective in a neighborhood of Madrid to promote local governance. *El Campo de Cevada* is a crossroads of networks and territories of digital dynamics and physical presence. Those who participate in *El Campo de Cevada* network, create a process (software), and transform the physical space (his/her body, the collective garden, the basketball court, and other collaborative projects) to the "open hardware" or base that is the community. **Tactics:** Discourse/Narrative + Commons **Major stream:** Deliberative
Node: *Red latinoamericana de estudios en vigilancia, tecnología y sociedad (Lavits).* Lavits network aims to be a means of debate and exchange of knowledge and reflections on the technologies that allow the collection, storage, management and crossing of information,

especially personal data.
Tactics: Discursive/Narrative
Stream: Ironic

Node: *Digital Rights*
Digital Rights is one Latin American independent and non-profit organization founded in 2005 and whose fundamental objective is the development, defense and promotion of human rights in the digital environment. The organization's work focuses on three fundamental axes: Freedom of expression, privacy and personal data, copyright and access to knowledge. DR also gives information about PETs and forms of security information.
Tactics: Discursive/Narrative + Commons + PETs
Major stream: Agonistic

Node: *The Brazilian Internet Steering Committee (CGI)*
The CGI has the assignment of establishing strategic guidelines related to the use and development of the Internet in Brazil and for the execution of Domain Name registration, Internet Protocol (IP) address allocation and administration pertaining to the Domain Level ".br". It also promotes studies and recommendations on procedures for Internet security and proposes research and development programs to maintain the level of technical quality and innovation of Internet use.
Tactics: Discursive/narrative + Commons
Major stream: Deliberative

Node: *FGV DIREITO RIO's Internet Governance*
A Brazilian governance project that seeks to address the different processes of governance and regulation of the Internet, with the purpose of proposing suggestions that can be used to elaborate sustainable public policies and private practices. From this perspective, we analyze the governance and regulation mechanisms of the Internet and the development and promotion of strategies that allow individuals to become active and empowered subjects in the online environment. Associated with the FGV Superior Education Foundation.
Tactics: Discursive/Narrative
Stream: Ironic

Node: *INTERNETLAB Brazil*
An independent research center that aims to foster academic debate around issues involving law and technology, especially internet policy. Our goal is to conduct interdisciplinary impactful research and promote dialogue among academics, professionals and policymakers. We follow an entrepreneurial nonprofit model, which embraces our pursuit of producing scholarly research in the manner and spirit of an academic think tank. As a nexus of expertise in technology, public policy, and social sciences, our research agenda covers a wide range of topics, including privacy, freedom of speech, gender, and technology.
Tactics: Discursive/Narrative
Stream: Ironic

Node: *The MediaLab.UFRJ*.
Founded in 2012, MediaLab.UFRJ is an experimental and transdisciplinary laboratory housed at the Federal University of Rio de Janeiro (UFRJ) School of Communication. Coordinated by Fernanda Bruno, its research projects focus on the crossings of techno-politics, subjectivity and visibility. The laboratory also explores digital methods for data analysis and visualization in the field of Humanities. By experimenting with different languages, methodologies and conceptual perspectives in the production and propagation of our research projects, we aim to make the laboratory permeable to urgent social and political issues.
Tactics: Discursive/Narrative
Stream: Ironic

Node: *EM REDE*
This is a Brazilian forum for reflection and discussion of topics such as Free Culture, Remix, Open Science, P2P Economics, Network Politics, and other issues related to new forms of organization of institutions and circulation of intellectual goods related to current electronic networks.

Tactics: Discursive/Narrative + Open Code **Major stream:** Deliberative
Node: *Codingrights.org* Coding Rights is a Brazil--based women--run organization working since 2015 to expose and redress the power imbalances built into technology and its application, particularly those which reinforce gender and North/South inequalities. We perform multidisciplinary research to hack public policy in order to reinforce human rights values into the usages of technologies. **Tactics:** Discursive/Narrative + Digital Mass Hacktivism **Major stream:** Agonistic
Node: *Calango Hacker Club* Based in Brasilia, the group defines that all information and knowledge should be free; "We seek to understand the fundamentals of systems and any other tools that can teach and broaden the understanding of how the world works. We believe that access to information and knowledge must be total and unlimited. Our structure is formed by a model of decentralized authority, promoting the transference of all decisions, knowledge, and actions. Our Hackers are evaluated according to their talent (Creations/Modifications) and not by any other criteria such as academic degree, race, gender, religion, social status, or age. **Tactics:** Digital correct hacktivism **Stream:** Deliberative
Node: *Tsunami Democràtic* This is a protest group advocating for Catalan independence, formed and organized in the lead up to the final judgment on the Trial of the Catalonia independence leaders in 2019. It organizes supporters of the Catalan independence movement through the use of social media, apps and other online resources. There is no official description, but it uses a 'bespoke' Android app, along with a Telegram account in order to mobilize and organize demonstrations during the 2019 Catalan Protests. The app allows the Democratic Tsunami to monitor and give directions to individual protesters or groups of protesters while claiming that the user's location is approximated and obfuscated to avoid police tracking. The app also requires the user to activate it by scanning a QR code, a measure intended to limit activation to "stranges" in order to avoid infiltration by government authorities. For the same reason, users are allowed to invite only one other person to the app. While officially endorsing non-violence, the group has supported the occupation of government buildings and other protest acts, which were condemned by the Spanish government. The group also used similar language to the Hong Kong Protesters, urging protesters to "add up like drops of water" (See Minder, R. 2019, October 18. "Catalonia Protesters, Slipping the Reins of Jailed Leaders, Grow More Radicalized". The New York Times. ISSN 0362-4331. Retrieved 2019-10-18.) **Tactics:** Riots + Unrest **Stream:** Despair

Source: The author

Chapter 6. Surveillance and personal data: connecting the points

In this part, we reconsider the main surveillance ideas presented in the theoretical framework and the analysis of the governance of personal data from the last Chapter.

To do so, it is important to recall our concept or understanding of surveillance. Surveillance is the continuous socio-technical interaction or activity addressed to collect, process, and refine information from/to certain objects with concrete or diffuse purposes. This phenomenon ranges from the mediation of power through the gaze and the self-discipline of subjects (panoptic metaphor), to the gaze as a site of nodal power (rhizomatic assemblage metaphor) that mediates the transition between exceptionality and normality circumscribed to the objects of surveillance (the watched).

As surveillance is connected to the panoptic and the rhizomatic assemblage, it also consists of the regulation of life cycles, development, and growth of individuals (biopolitics). Also, it entails the management of populations with the aim to constitute and sustain the dispositives that coalesce and operate the techniques to select, sort, classify, categorize and govern the heterogeneous "mass" of people (governmentality). Thus, surveillance does not equalize a relationship of power between surveyors and surveilled. It also entails a relation of power that produces different fronts of reaction and resistance to the mechanisms of governmentality.

Considering the definition, we can establish three core ideas: there are modes or metaphors to operate surveillance, there is specific management of individuals in a population, and there is resistance derived from power relationships. In turn, those ideas can be reformulated to create connection points:

1) How the surveillance metaphors from the theoretical framework can be incorporated and interpreted in the governance of personal data? (Section 6.1)

2) How personal data affects the management of subjects and populations? (Section 6.2)

3) Is it possible to think in new forms of resistance and accountability besides the explored civic agency streams? (Section 6.3)

The points are also explained because they allow to establish a common ground to reach our study objectives. By answering those points, it is possible to assess the management of individuals' autonomy as well as the power

asymmetries between watchers (data processors) and the watched groups in the population. Moreover, the latter point explores whether resistance can be exercised in ulterior paths, in order to reach greater levels of people's legitimacy.

To answer the three points, we do not intend to formulate a fixed image regarding the actors and the governance of personal data. Rather, the points try to update the surveillance concepts from the theoretical framework with complementary analysis and accountability findings from the last Chapter 3. Besides, the connections might be reworked by scholars researching more cases and can be used by prospective studies on personal data and surveillance. Let us answer the three points separately.

6.1. Surveillance metaphors and personal data

As we have seen in the last Chapter, the digital persona stems from psychology and is considered as a model used by the individual to construct a public personality (Clarke, 1994). This model is based on data transactions and is intended for use as a proxy for the individual. Thus, one individual can have different personas or proxies. However, the surveillance digital flows can replace the individual capacity to construct his/her persona. Also, the individual can lose control on that construction as it also depends on the continuous interaction with the social domain. In this domain, the management of people is exercised through the abstraction of data-doubles and by data that ensemble "dividuals" (Deleuze, 1995). In the surveillant assemblage, the digital persona can be sorted, rendered, fragments, combined, recombined, discarded, categorized, or even ignored by the molds of observation and the gazes that interact in the "house of mirrors" of informational flows (Johnson & Regan, 2014). Thus, surveillance can replace and recreate the original identification and context of individuals.

If we go to the past, the abstraction, refinement, use, and meaning of individuals' information was reformulated with the first writing revolution after the consolidation of city-states five thousand years ago. But now, the intensity and the pace of that recombination are accelerated thanks to the tools and electronic devices of the current informational world. In the last millennia, the means of the message was determined by the content of communication. Nowadays, the technological means determines the content. Throughout history, when humans wanted to convey a message, the means (walls, paper, letters, books, radio, television, etc.) were created to deliver that message. Those means already highlighted the need for communication and to the ability to represent people. With the current informational tools and the advent of algorithms and automated tools, the channels or the means redefine communication itself and the very humanity of people in a deeper pace.

As cyborgs in which biological parts assemble with technological devices, our interactions are redirected by the platforms, websites, and machines that permeate every digital interaction. The advent of programming -coding, rewriting, copying and creating-, and the operations in the backend layer of electronic platforms are perhaps the second writing revolution in human history. Five thousand years ago, for example, the first Akkadian and Sumerian writers were especial and talented men that worked in the first city-states to represent the title of lords, the accounts of the economy, the rites of priests, and the hymns to gods (George, 2002). Nowadays, the new "writers" have the skills to teach machines, configure systems and manage information for the sake of every human activity. At the dawn of civilizations, writing was a matter of high-policy, something related to social elites until the Enlightenment revolutions two centuries ago. During human history, almost every man and woman that lived on this planet was an illiterate person. In the same allegory, the new writing revolution of our time is concentrated in a body of technicians instead of being a matter of universal access. And even if this skill becomes popular in the future, coding and machine languages will continue to be the means through which we shape the content and the social relationships of people.

Yet, broader access to the "secrets" of technology would not redefine necessarily the forms in which power is distributed. In the same form, the universalization of writing did not represent the end of social dominion and subjugation of entire populations in past times. Thus, even if we reach a point in which technology can redefine the fate of humanity, let us not forget that technology per se does not exist and this domain is also permeated by power, politics, clashes, and cooperation between people.

In that sense, the panoptic disciplinary effects started to focus on dispositives to spread the power of "seduction" (i.e. gamification) and the transparency of people in the current digital architectures (see the idea of slides of visibility in the last Chapter). Surveillance metaphors nowadays are not focused exclusively on the impulsive energy to punish and correct behavior.

As attested in the market analysis, strategies centered in users, privacy by design, risk analysis, and security of information systems converge in a paradigm of surveillance that hinges on the "care of the self", in caring our reputation and image, rather than in promoting hard disciplinary means of control. One can even argue that the state regulations to protect personal data are the legal envelope that surrounds the market strategies to handle and process data. Market players are organizations that collect, match, and deliver data to third players with the purpose to administer the flows of data. Market players monitor the volume, the noise, and the interactions of people without a priori goals of social control.

Rather, their monitoring is similar to the one expressed by Zuboff (2019) in her ideas of instrumentarian surveillance. Instrumentarian means that watchers are more concerned about watching the interactions rather than constraining them. For them, it is better to see the pipeline full, no matter the content of the flow and the origin of the liquids, than empty. Surveillance, then, would be more connected to the observation of performance and productivity to create more data (from labor to entertainment), rather than to discipline souls and biological bodies. Yet, the latter dimension is still present. In doing so, information that would be banal or "futile" (like many messages from common people) has reached, for the first time in human history; the status of a value per se. Surveillance has obtained a retro alimentary logic. Watching has reached a self-perpetuation ending. To use a science fiction metaphor from Philip Dick, the electric sheep (the cyborg) dreams about another electric sheep that is also dreaming.

This logic is the continuation of a historical process in which every social activity has reached a point of auto-poietic production or, in rough terms, of self-perpetuation (Luhmann, 1986). For example, arts has reached the status of a valuable and independent practice. Despite the ever connection to the social and politics, arts has symbols and materials that constitute a finality per se (Rancière, 2009). In the same logic, informational activities have reached a self-ending function as they feed internal demands to collect, analyze, and produce even more information. Data generates data. Its production demands even more data to analyze the previous one, which in turn needs to be matched and recombined with other one, restarting the circle.

But the self-referential process is not limited to data and surveillance. Surveillance is being complemented with another process called differentiation. Since the informational revolution in the last decades, "differentiation" is similar to the Deleuzian becoming or potential capacity to create something new. It is a process in which every social domain gives birth to a subfield that in turn constitutes itself as a new epistemological and social domain (Luhman, 1989). Like a branch that stems from new branches, the social domains are increasing in number and volume. The universe is expanding and the celestial bodies are accelerating to the borderlines of the cosmos in a process called inflationary expansion. In a similar way, the social objects and informational fields are also increasing and accelerating to produce new ones.

In that process, the new differentiated objects and data might become detached or distant from previous fields. It seems that, despite the hyper-connectivity and the production of new data, one challenge consists of giving an overall sense to connect the production and volume of data. The idea of a super-panopticon is now too short to catch up with the bulky information produced every day. To do this job, machines and automated procedures deploy provisional tools to interpret targets and data sets, seeking to simplify and reduce the

complexity of the information. Yet, those tools create new domains of specialization, social knowledge, and technical expertise as verified in the last Chapter. Those characteristics, in turn, contribute to accelerate the inflationary expansion of entropic data and as, in the end, they call for new procedures to interpret it.

Thus, the first driving force in surveillance nowadays goes beyond the theoretical ideas of social control in the surveillant assemblage as commented in the first Chapter. Rather, it correlates to entropic directions of differentiation and to the demands to analyze new data, especially through the work of giant data processors that constitute the first domain in the global economy. One mobile phone has the same ability to process data as the analogic-bureaucratic intelligence agencies during the Cold War. Today, larger amounts of data are being produced in short periods. And to the problem volume, the quality and integrity of data are inversely proportional to the capacity and velocity to process it by electronic tools. The more data is produced, the more we need tools to clean information and listen amidst the noise of data.

The second driving force in surveillance is the response from markets and states to orient and interpret the production and monitoring of data. Insofar as they cannot control all the information and handle all the tools to analyze personal data, they have started to direct their efforts into the sources of information. In the last decades, they started to focus on the recipients of information: individuals. Beyond being a source of production and labor, a population has become, at the same time, a reserve of information that can be better exploited for the benefit of the dataveillance assemblage. This exploitation does not necessarily take the commodity form. Populations are also potential sources to feed the pipelines of information beyond the ideas of traditional governmentality. Data subjects are valuable because of their constitution: they are subjects *of* data. The use of databases is as valuable as the natural resources to determine the wealth of nations in this century. As attested by the market governance in the cases of study, the expansion of data conglomerates the capacity to manage populations is perhaps the new frontier to decide the future of humanity as subjects or individuals.

6.2. Personal data and the management of subjects

In the analysis of surveillance and intelligence (Chapter 4), we mentioned that subtle discipline and biopolitics converge to administrate subjects and to regulate the distribution of power in the sociopolitical order. Biopolitics is based on biopower, a dimension of power exercised traditionally over physical bodies. Its foremost theorist, Michel Foucault, expressed this dimension as a regulatory dispositive aimed to regulate individuals by their individuality. Since the

industrialization of western societies, Foucault described biopolitics as “new technology of power […] [that] makes use of very different instruments.” (Foucault, (1979) 2008, p. 242). In Foucault, biopolitics focuses on the body and serves to regulate biological procedures: reproduction, birth, mortality, health, life expectancy, longevity, and all the conditions that regulate them (idem: 139). In short terms, through biopolitics, individuals become tools and instruments of power.

In that sense, the very idea of active citizenship and individual autonomy is shifted by the mechanisms that allow biopolitics, such as the forms to regulate and administer personal data. For example, it is psychologically hard for humans beings to understand which and how much data is captured about them, how and why it is used, and what effects it has about their lives in the complex interplay among users, organizations, algorithms, and regulations (White & Ariyachandra, 2016). Yet, if the individual is not aware of the whole digital ecosystem surrounding her, it does not mean that other organizations replenish their power and social position thanks to the information obtained from unaware individuals. On the other hand, it is crucial to recognize the subject is not totally passive. Any idea of autonomy should be drawn from this point.

Autonomy can be combined with active forms of interaction, as in the case of deliberative and agonistic tactics of resistance depicted in our cases. The civil agency can be executed even when it seems that individuals are mere instruments of power. However, Iaconesi (2017) describes how spectacularized information visualizations (also called "data smog") distance people from their abilities and responsibilities to understand relationships between the multiple ecologies in which they live, and the possibilities they have. This social distance is amplified as individuals are exposed to content they potentially like. The more people are clustered and categorized in proxy categories in the governance of personal data, the more they are enclosed in informational bubbles. Ultimately, these categorization tools could implicitly reduce "otherness" presence from our reach.

This brings on a series of controversial effects, such as the diminished sensibility to and acceptance of diversity (Bozdag & van den Hoven, 2015), rising levels of cognitive biases (Bozdag, 2013), diminished tolerance, and social separation (Boyd & Crawford, 2012). During the physical social distancing imposed in our cases during the pandemic crisis of 2020, for example, social relations were restricted to digital interactions that reinforced the exposition to previous clusters of information, increasing the feeling of belonging among ‘equals’. Meanwhile, the segmentation reinforced previous differences and inequalities. Whereas many students watched virtual classes and some workers stayed at home offices, digital gaps to access online education and the precarious jobs of many (some of them attached to digital apps) were as usual as in normal times. For those who lost relatives and friends in the pandemic, even the streaming

of funerals exemplified that material constraints and necropolitics were reshaped by the digital hyperconnectivity and social distancing. Those outcomes also prove that even exceptional moments reinforce previous normalized differences (of access, share, and use of technology) that cut across society, from life to death.

Moreover, informational bubbles and the reduction of social diversity in individuals' interactions may bear the possibility that individuals progressively inhabit a controlled infosphere, in which a limited number of subjects can determine what is accessible, usable and, most important of all, knowable. This power asymmetry also implies the fact that users can systematically be unknowingly exposed to experiments intended to influence their sphere of perception to drive them to adopt certain behaviors instead of other ones (Zuboff, 2019). Yet, one might still be skeptical about the apocalyptical visions that utter a sort of alienation and people manipulation at the advent of new technologies, such as during the rise of television and cellphones in past generations.

However, what is different today is the mentioned capacity to encapsulate users on information bubbles that go beyond material devices and personal choices. Despite the ability to choose alternative sources of information, or to turn off cellphones, there is less room to escape from the informational flows based on personal data. Individuals became not only targets but also sources of information. The online interactions redefine our roles as subjects of rights, services, and actions. Thus, as seen in the previous chapter, the tension between autonomy and control of individuals can be elucidated from power clashes between regulators, markets, and users in the governance of personal data.

In that governance, individuals are not separated from the social context and nature. The flows of information are as vital as the water and food to live in our current societies. Following the evolution of data governance, the traditional economy of scarcity (of material goods) has been supplemented by a new economy of abundance (of immaterial goods). Sharing and distributing material artifacts usually decreases their value but sharing and distributing immaterial artifacts almost always increases their value (Martínez Cabezudo, 2014). This context transcends the labor horizon, affecting our mutual interactions, our sense of own reality, and our interactions with reality itself (Jandrić et al., 2019). The digital fusion of material and immaterial production reaches well beyond the economic sphere to directly address the cultural, the social, and the political. In that sense, this type of production expands biopolitics because it directly affects life as a whole, producing not only immaterial goods but also concrete relations and ways of life (Hardt and Negri, 2004).

Thus, it is not necessary to consolidate breakthroughs such as quantum computing, natural language processing, ubiquitous neuronal networks, and non-supervised artificial intelligence to realize that we have arrived in the age of digital

biopolitics. Its current phase, the 'biologization of digital reason' (Peters & Besley, 2019) is a distinct phenomenon that is emergent from the application of mechanical reason to biology and the biologization of digital procedures. Indeed, the promise of those technologies works like utopian dreams to justify a technological Manifest Destiny based on the amalgam body-machine to "save" humanity from social problems.

Moreover, we do not need to move to science fiction scenarios and dystopias to realize that current personal data is the extension and redefinition of biopolitics. Digital data reflects not only biological procedures (sex, gender, age, ethnicity, family, class, social relations) but it also constitutes new sources of differentiation attached to the body and beyond the body. Data fragments can be rendered and recombined to give rise to new forms of representation that are not strictly attached to an essential individuality but to its becoming. In flexible data flows, bodies and subjects are valuable by their imminence rather than by their immanence or essence. Even if personal data protection rules obligate consent and individual rights to process data, the amalgamation of informational systems, the renderization of algorithms, and the refinement of data can be potentially worked to reinforce the re-creation of "dividuals", individuals disconnected from their original sources.

Thus, if in the last century surveillance was closely related to suspicion and dissidence, in which individuals needed to hide something to avoid surveyors, today those logics have been added by capillary networks adapted to each user. One can think "I am a normal person and my data does not matter, I have nothing to hide". Yet, the capacity to instrumentalize people nowadays works at the individual level. What each person does (or not) matters to build a broader image of populations. Besides, personal data also matters to redefine the very idea of individuality at social scale. Today, there is accurate potential from automated surveillance to reach each person, in which the techno-social interaction between persons and machines allows or closes different opportunities to understand the world, and so to live. Thus, giant data processors like Google and Facebook always strive to deliver or maximize the personal "experience" and the performance of each user. Surveillance works thanks to the differences among the bulky data. In that sense, biopolitics now replaces the mass administration of biological bodies as it combines new forms to allow the identification and validation of fragmented subjects. For instance, in national security realms and market domains, the recombination of data and the correlation and matching of data fragments is even more important than the individual itself in terms of observing and managing a population.

Thus, biopolitics has also enabled to focus on individuals as a mass, allowing mechanisms towards the conduction of life processes with the support of new forms of knowledge that take into account probabilistic and statistical judgments

(Van Dijk, 2014). In that sense, personal data systems, as mechanisms for the sake of identification and assessment, are part of the set of networks of power that constitute the architecture of a performance society. It becomes a way of government and organizational culture in which the information flowing in the digital architectures is what sustains organizations themselves. Thus, the governance of personal data entails not only the channels or forms of power, but it also conditions the social stratification, the social systems, and the social position between players. Biopolitics, in that sense, redefines the prefix "bio", from pure organic bodies to power oscillations that redefine the entire material-immaterial world. Biopolitics constitute the amalgam of cyborg-bodies and overpasses the Foucauldian governmentality definition, the set of dispositives to administrate a mass of people, to alter even classic ideas of reality.

One of those ideas comes from the "hyperreality" by Jean Baudrillard ((1981)1994). According to him, since the 1960s and 1970s, the mass culture and information era were part of a social development in which there is not a reality we can touch and reach because what matters is the encapsulation of certain parts of realness (selection) and the delivery and marketing of those parts as they were "real". To Baudrillard, the symbols of reality and their simulation substitute reality and it cannot be fully grasped because of those selection procedures. The "desert of the real" (idem, p. 69) is the world we live in. However, in the recent decades, we have seen the rise of probabilistic and statistical judgments, as mechanisms for the sake of identification and assessment. These new tools are part of the set of networks of power that constitute the architecture of a continuous performance society that alters previous ideas hyperreality as a continuous simulation.

Nowadays, surveillance does not refer to divisions and criteria to distribute symbols that emulate reality back to individuals. It refers to assuming the insufficiency and indeterminacy of hyperreality. In other words, the more data surveillance collects from individuals, the more it uncovers that there is to know, which makes people recede even further into their massive mystery and unknowingness. Far from marking the limit of the dataveillance, this apparent paradox is simply its functional principle. The aim of surveillance through personal data nowadays is not modeling and understanding an external object or to simulate reality to a mass of bodies. Its aim can be the endless reproduction of objects' statistical indeterminacy and opacity as the protocol of the system continuing operation. "We can thus see why in hyperreality the two inevitably converge: power (as vigilant connectivity) and resistance (the silence or recalcitrance attributed to the masses) belong to the same logic of simulation" (Kaplan, 2018, p. 186).

In light of that, the myth of our era consists of the illusion that data can speak for itself. Surveillance produces a new hermeneutic cycle to interpret reality and proclaims that data needs more data. However, this assumption never grasps

individuals or consists in a quest for more knowledge, because there is nothing to know (data is always incomplete) and no sense in knowing (to give cohesion and coherence to reality). There is no necessity to know and give sense to a reality comprised of data fragments as surveillance becomes tautological. In that myth, the main object big data processors can do is to declare they can interpret the world and people without their mediation and resistance by finding "relevant" correlations.

In other words, the current surveillance is an auto-poietic cycle in which inefficiency inhabits its efficiency. Its cynical meaning, as expressed by Kaplan (2018), disallows a ground for reality representation and undermines subjectivity and agency. Contrary to surveillance interpretations based only on self-discipline and social control, or in the specialization of bureaucratic organizations (Dandeker, 1990), surveillance now brings up a symbolic efficiency that enables a self-referential expansion by the differentiation of objects and the inflation of informational bubbles. In that path, surveillance continually marks the unity of cognition with data deficits that must be overcome. As the deficit will ever persists, because data is never enough, the operation of surveillance constitutes an efficient system indistinguishable from endlessly recurring failures. As being efficient attaches to being inefficient, surveillance might become immune to accountability efforts that expose the failures and the inefficiency of powerful surveyors. Yet, in the endless hermeneutic cycle that reshapes reality and technical efficiency, power is not equally distributed and clashes emerge reworking the notions of resistance to challenge surveillance, once again.

6.3. Personal data accountability and further resistance

In the previous chapter, the analysis of accountability mechanisms in the governance of personal data was conducted in three domains: state regulations, market strategies, and civic agency strategies. We found that the last one has the potential to enhance a new form of governance through streams and strategies of resistance. As this study suggested, state-rooted regulations and market strategies have improved some accountability mechanisms, especially those actions regarding answerability and enforcement principles (such as defining standards and norms to handle data) and even transparency (as in the case of transparency reports and accountability of algorithms). Yet, in an overall sense, those domains have serious limitations to bring responsibility to organizations that need to assume duties and missions to use data.

Besides, it was mentioned that a fluid and complex accountability network, in which organizations are accountable to everybody, could create a scenario where "nobody" is deeply accountable to each other. Shared responsibilities to protect and manage personal data can create a diffuse concept or vague

commitment that are required to handle and process data. Thus, a deep commitment to preserve individual autonomy and to replenish the asymmetry of power -between data processors and data subjects- depends on a series of actors, from the state to companies and people.

However, when it comes to reinforce the power position from data subjects, each of the three domains presented critical points that can be summarized as follows.

In the first domain, data protection rules have been enshrined in Spain and Brazil in the last years. Those regulations are extensive in scope and purposes, but they could be deemed as a market-oriented reform to introduce principles from Privacy by Design, risk assessment, and user-centered management. Those topics were deemed as ideal accountability principles within market organizations and business environments as attested in section 5.2.

In market organizations, however, criticism remains as market principles such as Privacy by Design does not necessarily address methodological aspects of system engineering, complete data lifecycle, and reversed anonymization content. Moreover, it has been pointed out that the new regulation (and new market self-supervision), could be similar to voluntary compliance in industries impacting the environment. Despite the scheme of fines and enforcement, the efficiency to implement accountability may differ in every company. Some critics have pointed out that certain business models are built around customer surveillance; therefore, voluntary compliance is unlikely (Rubinstein & Good, 2013).

Thus, it was essential to analyze accountability practices in a third domain: the civic agency. Here, institutionalized and informal strategies give more importance to redefine the asymmetry of power between data subjects and data processors. Whereas the first two domains may conceive the public as policy users and market consumers, the civic agency defines the citizens as politically active agents. Citizens addressed as consumers of laws and products endorse a poor notion of governance, where individuals are passive subjects and organizations are mere suppliers of correct norms and good services.

By considering data subjects as active and autonomous subjects, the civic agency has increased the scope and the strategies for accountability. For instance, deliberative and agonistic strategies are just some examples that reinforce free access to information that in turn might replenish digital informational power. Moreover, these actions are in the front line of technological developments such as Open Codes and Privacy-Enhancing Technologies or in specific interventions such whistleblowing that could mitigate intrusive surveillance. A strong civil society lying outside the power of state and market players is important to influence public accountability. This domain is critical to demand answerability (i.e. to formulate recommendations to the correct use of personal data) or spark

enforcement (like pressing justice courts to take actions after the misuse of personal data). From the streams of resistance, we learned that it is not possible to think in filling the gaps of accountability, like holding governmental agencies accountable before the public interest, without the role of civic agency. A comprehension of the social, political, and economic dimensions related to accountability must be oxygenated also with informal strategies that expand the public sphere beyond legal rules and institutional boundaries.

The multitude cannot be labeled as purely good or evil. Yet, tactics of necessary confrontation are alternative paths that can foster legitimate policies, promote awareness, and relocate informational power in favor of data subjects. From the despair stream, we learned that resistance is an array of attempts to construct new realities –even if these attempts are a provisional set of informal practices- bargaining power against hegemonic political forces. In that sense, civic agency strategies have open goals, but they can be edited to mitigate the regression of politics into hierarchical forms such as technocracy or oligarchy, which in turn may offer a mask for inefficiency and corruption.

The impact of the contemporary civic agency in both countries is still debatable and open. This domain calls for further measures to guarantee privacy safeguards and to empower personal data subjects. However, at the same time, is important to recognize that even the civic agency streams of resistance have limits when it comes to relocate the asymmetry of power between data processors and subjects.

One of those limits is that the conjugation of the streams is contingent and depends on a set of variables, from agency to structural levels that only appears in specific times in history, such as in the cycle of protests after 2011 in Spain and 2013 in Brazil. Other limit regards to the cooptation of resistance strategies by counter-resistance reactions that might curtail the energies and tactics from the multitude. We mentioned the tactics of disinformation and counter-information in the ironic stream, and the neutralization of the despair stream. Also, every action of resistance can return to their promoters as a "domesticated" product (i.e. the use of commons from the deliberative stream to build commercial digital platforms that reinforce the market position of big data processors).

Another limit stems from the epistemological understanding of resistance in terms of objects and orientation. If resistance has no clear endings, as attested in the idea of open becoming and social experimentation, and because of the non-essentialist characteristic of the multitude, it means that the civic agency cannot be completely tamed and dominated by stronger actors. Yet, it also means that any attempt to propose an ulterior and general path to resistance would also be controversial. If the multitude has not necessarily a concrete ending (i.e. to

promote structural changes to increase the power of data subjects), this entails resistance as an ongoing or continuous process of reaction that never ends.

Yet, since history is not eternal and human efforts are finite, other paths and alternative endings need to be developed to rethink resistance and the array of tactics that challenge surveillance. If data subjects want to deeply alter the asymmetry of power against data processors, deeper paths must be carven to orient the collective action of the multitude to promote further outcomes. It is not enough to break or disrupt the digital flows of data and create spatiotemporal gaps between the watchers and the watched as affirmed by Ball (2005).

In that sense, in this Part we have seen different actors from the multitude that challenge surveillance, from the micro to the macro level of politics. We coined a model to interpret and analyze the different streams of resistance and offered a sample of actors. Yet, when those actors engage to counteract or resist, so what? Is there any major orientation in the heterogeneous reactions from the people to redefine their position as data subjects? Those are important questions to think resistance beyond contingent and heterogeneous tactics that change politics. We mentioned that ultimate goals for the civic agency cannot be understood in essentialist terms, neither in the sense of pointing a definitive direction. Yet, we can propose major conditions to orient resistance. This is because the substrate in which resistance moves nowadays is different from the 1960s and 1970s, or even from the 2000s. Different structural conditions demand to re-program macro resistance in major forms, and this will be the focus of the last part of the study.

Part 3 consisted of Chapters 5 and 6. In Chapter 5, we introduced personal data notions and dataveillance. Moreover, we analyzed the accountability mechanisms that have emerged to restrain data processors since the Internet expansion in the 1990s to the present time. We have explored three domains: state regulations, market strategies, and the civic agency. To base the analysis, the chapter used primary sources from data companies, media articles, jurisdiction and laws, and specific literature in each country. The three domains were interpreted under a governance analysis, in which they show interdependence but at the same time specific roles to manage data. For example, state regulations have been promoted to guarantee data rights (access, rectification, consent, opposition, forgetfulness, portability, etc). Data Protection Authorities can also foster answerability, transparency, and recently they are obtaining enforcement capacity to decree fines and administrative sanctions. In the case of the market, accountability has been formulated through responsibility, in order to assume duties and obtain trust to process data. Also, it has promoted passive transparency, releasing information about the cooperation with enforcement and state agencies. In the case of civic agency, the multitude of people is considered as a heterogeneous domain that can foster accountability especially when it comes to replenish the asymmetry of power between watchers and watched, between data processors and data subjects. In that sense, the multitude can use strategies and tactics that range from rhetoric/arts, cooperation, confrontation, and high conflict.

In Chapter 6, we returned to the concept and theory of surveillance to connect the main findings in Chapter 5. The points of connection are regarded to surveillance metaphors such as the panoptic and rhizomatic assemblage, personal data and the management of subjects in populations, and further resistance in the governance of data. We also expressed that accountability here depends on proactive measures from data processors, and sometimes, from the collision between state and market actors. On these fronts, responsibility can become fuzzy and transparency can lose effect if detached from organizational and ethical changes. Hence, the accountability mechanisms have limited potential to preserve individuals' autonomy and recalibrate the asymmetry of power between watchers and watched. We also mentioned that surveillance uses personal data to elaborate a new reading (hermeneutics) from society and reality as it differentiates in a self-referential cycle. In that sense, data becomes valuable beyond initial biopolitics and commodification definitions. Data becomes the new “currency” of this era as data flows reconstitute power and even individuality. Those changes represent serious challenges to the civic agency and resistance, especially when this front uses double-edge swords such as non-definitive orientation and heterogeneous tactics that might become diffuse and hijacked by hegemonic actors. Therefore, we expressed that further resistance needs also to be reprogrammed in the structural level of politics, on a major scale.

The next Part 4 is the last step of this journey. Here, we rethink resistance through the idea of metanarratives, the universal and common paths that can be reestablished to guide politics and human actions. This allows formulating big principles that in turn serve to revisit accountability, from reformative to radical principles. This part redefines accountability as a relationship between authority and legitimacy, exploring new mechanisms to restrain power in surveillance and replenish politics in a broad sense.

PART 4

"Postscript" on the societies of surveillance

"Seguir siendo humano, albergando ilusión en el alma, deseos frenéticos en el corazón, en medio de esta pesadilla, eso le pido yo a los dioses."

Manuel Vilas

In the previous chapters, we have seen different actors that challenge surveillance in the structural (macro) level of politics. We also offered a model to interpret and analyze the different streams of resistance. Yet, the substrate or the major conditions of the structural level in which resistance moves nowadays is different from the past. Macro resistance nowadays is different from the 1960s and 1970s. What has changed since then? In other words, different structural conditions of surveillance demand to re-program the major conditions and paths of resistance. In that sense, this last part complements the previous chapters showing the importance to construct general paths, metanarratives, to orient the collective action from the digital connected-multitude. Thus, we formulate a sort of "postscript". It is a final synthesis and deeper attempt to relocate the asymmetry of power between watchers and watched. This is also a prospective attempt to stimulate the autonomy and agency of citizens, as well as a final remark to amend the analysis of intelligence and personal data. We start addressing the forms to understand metanarratives, giving three models or examples. Finally, based on the metanarrative models, we revisit the concept of accountability to expand the legitimacy of politics in a broad sense. This expansion is explained because resistance in the structural level is not restricted to surveillance, as explained in the last parts. Furthermore, metanarratives expand beyond our cases of study because they encompass all politics and the entire humanity.

Metanarratives for resistance

Metanarratives are great stories that orient history and humanity. At this level, time and social actors interact to follow a common direction. Metanarratives establish the direction and give meaning to collective action in historical, political, and philosophical terms. In most of history, religions were examples metanarratives that guided humanity. In monotheist traditions, the origin of human beings, as well as their destiny, pointed out to God through the idea of reconciliation, paradise, or the promise of salvation. In not monotheist traditions, human destiny was not fixed, either by the idea of coming reincarnations or

reconciliation with the universe in a state of awareness and fusion with nature. Religions and faith traditions are not separated from politics and they influence each other. Even when not secularized regimes or religious leaders invoke divine entities to evaluate their actions, the interaction between people, and between public institutions, are the main channels to promote social changes. All religious thinking might begin with God or divine entities, but it also must be worked down to man (humans). Faith and tradition are embedded in people actions, but the role of metanarratives in the realm of politics must be checked down on Earth. Thus, metanarratives are not incompatible with faith. But they also should be worked in political terms, in the world between the people, so as to orient the path of concrete historical events in societies. In that sense, rather than a cutting division between the divine and the mundane, it is possible to reformulate the base of metanarratives so as they can be mobilized by different beliefs and secular actions. Metanarratives can be reshaped as overall paths that guide the beginning, the means, and the destiny of history to generate individual and collective actions.

The beginning, the means, and the ending are the basic elements in metanarratives. In philosophical terms, those elements can be translated to these basic notions: ontology, modality, and telos. Ontology means the essentialist part of things and actors, it answers what and who we are. This answer is the departure point to construct projects and redefine our political world. Modality, in rough terms, is the becoming, the process of being, and the transformation. In politics, modality is the mode in which we travel in the great road of metanarratives. For example, normal politics such as the use of personal data is part of modality; it expresses the becoming, the gradual transformation of people through continuous interactions with their data every day. Finally, telos is the destination, the point of arrival. Telos is the station that we aim or the condition that the metanarrative seeks for. This is the utopian component of many political metanarratives as some of them aimed a new era, a time of quasi-salvation, or a “perfect” society.

The tension between the three philosophical parts of metanarratives (ontology, modality, and telos) is the tension between promise and actualization. It means playing with fundamental ideas that level up the pace and path of historical events. The tension between “who we are”, or the ontological actualization, and “who we are supposed to be”, the teleological principle of promise, mediated by a becoming process, are the steps to calibrate changes in political life. In that sense, the dialectical relationship between the parts of the metanarrative cannot be reduced to a difference between theory and praxis. Yet, this relationship might enhance the possibilities (current and prospective ones) to determine the actions of groups of people, such as resistance and counter-resistance.

Besides philosophical components, the basic components of a metanarrative can be translated using narratology tools. In narratology, metanarratives can also have three pieces: content (ontological meaning), forms

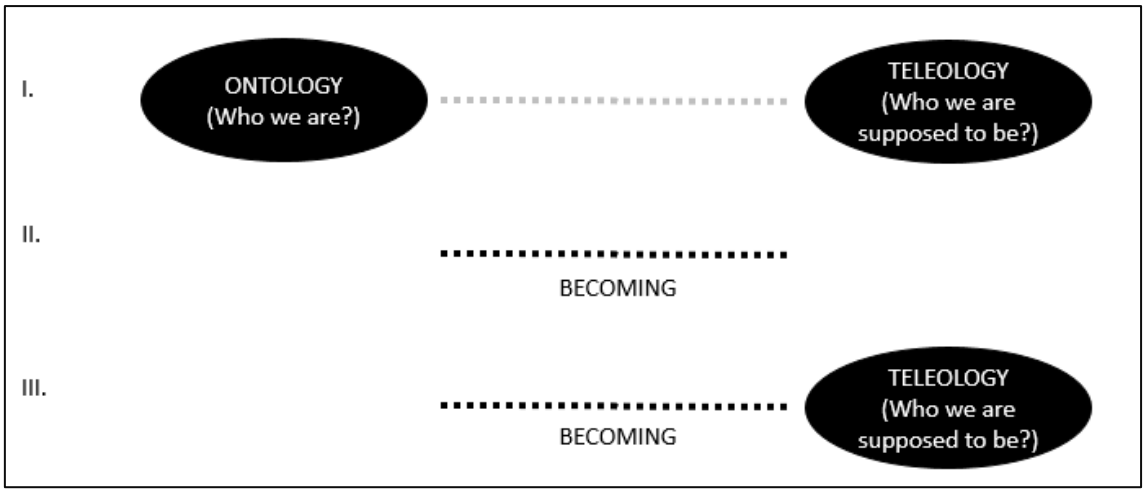
(modalities), and functions (teleological principles). In this dimension, narratives and metanarratives share a fluid logic of interdependence between content, form, and function. Linguistics and semiotics might relabel those elements as significant, signifier, and meaning. Yet, to simplify, the structure of a narrative can be expressed in terms of what a text/story is about (such as semantics and elements of significance), the form of the story (as modal components conveyed by the use of figures of speech, and stylistic variations from syntaxes and morphology), and what is the purpose of the story behind the story in terms of pragmatics (the functions that go beyond the semantics content and the form of the story, such as the conditions of production, and the socio-historical context of that production).

The combination of the narratological parts of the metanarrative (content, form, and function) interplay with the philosophical components (ontology, modality, and telos). In fictional terms, stories can create many combinations between those dimensions to create multiple signs, texts, messages, and even ideologies. However, as we attach to the political evolution of surveillance and resistance in the last decades, we limit those combinations with historical events to fill the content of metanarratives with historiographic interpretation.

Thus, the third dimension to analyze metanarratives comes from historiography. In light of that, even if historical and fictional narratives share many aspects (in terms of form and function), the content of history is based on past events that are commonly labeled as *facts*. Facts have layers of objectivity and subjectivity (interpretations) that are always attached. From the debate between objectivity and subjectivity in history, a central issue from positivist approaches in the 19th century, to the reinvention of History as a field of study in the middle years of the last century, history was replaced by a realization that both poles are always bargained to interpret facts and none of them overrides the other. A historical narrative with one hundred percent of objectivity is as impossible as a narrative based on total subjectivity; otherwise, it would not be a historical narrative based on facts.

In that sense, combining philosophy (ontology actualization, the modal becoming, and the teleological promise) narratology (content, form, and function), and historiography (historical conditions and context to produce a political path), let us present metanarratives ideal models based on those fields in order to analyze and deploy the major ground in which resistances can be conducted.

Figure 20. Three metanarrative models for resistance:



Source: the author

On philosophical and narratological terms, all the components of a metanarrative can be present (ontology/content, becoming/form, and teleology/function. Yet, due to historical constrain factors, the metanarratives that have existed emphasized or lacked some components. The first model emphasized the first and last components. In turn, in the second model, only the becoming/form component is present. Finally, the third model tries to add a teleology/function to the second one. Let us explain the reasons, characteristics and examples of each of those models below.

I. Icarus model

In the first model, the metanarrative aimed to congregate the full version, embodying the three philosophical components (ontological actualization, the modal becoming, and the teleological promise). In terms of content, one can exemplify this model with Enlightenment ideas from the 18th century, and the classic dialectic materialism rooted in Marxism from the 19th century. For example, the social contract of Locke and Hobbes, to whom overthrowing the government was legitimate in case it does not actualize the promise of security. For Rousseau, resistance was also legitimate to achieve more equality (Burgos, 2016). Moreover, classic dialectic materialism ideas inspired the implementation of real socialism in historical events such as the Russian revolution in 1917 and the Cuban revolution in 1959. Political factions and revisionism are inherent to Marxist theory and praxis because dialectical materialism is the philosophic product of class struggle (Lukács, 1969). Yet, in these events, the vanguard presented by revolutionary leaders was the engine of resistance (Benton, 1984). Moreover, intelligentsia or intellectual elites were able to introduce radical changes in History, guiding and

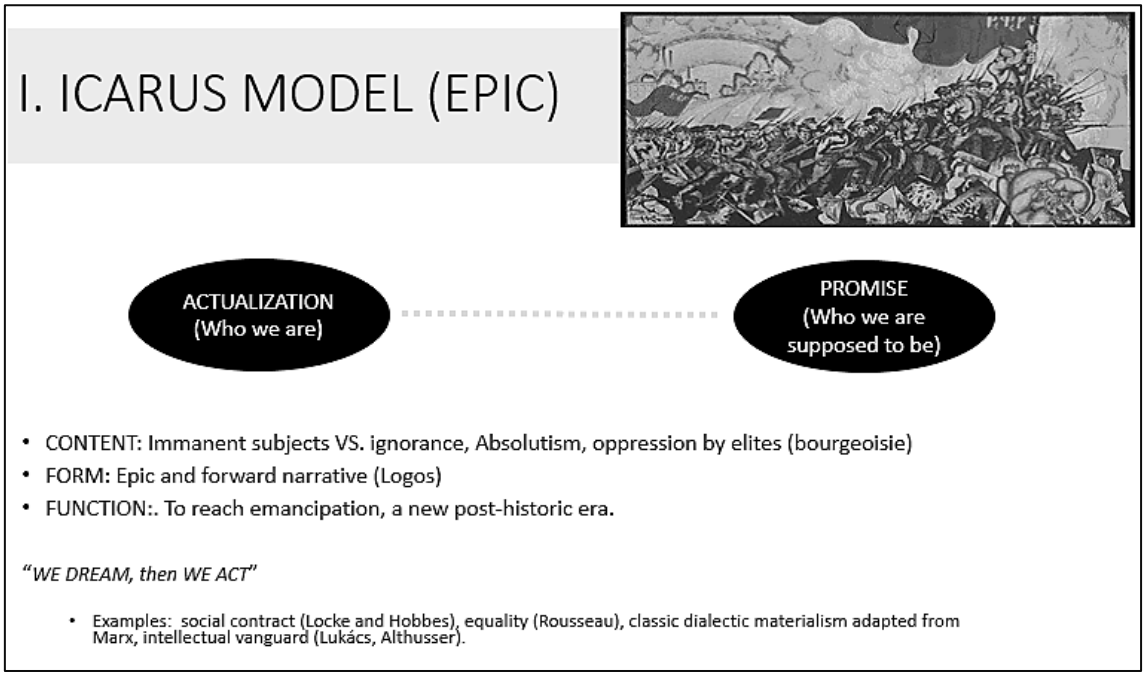
promoting social transformations to the proletariat. Those historical ideas can be considered as examples of content that filled the three parts of a metanarrative.

In terms of form or modal becoming, those metanarratives shared a vision of linear time in history. In other words, their form relates to an epic and forward narrative based on "logos", the reason, stemmed from the idea of scientific-technological progress, or the notion of class struggle as the engine of history. In terms of function or teleological promise, either in terms of social contract or socialist revolution, these metanarratives aimed to the emancipation of powerless subjects, and the achievement of a new post-historic era for the sake of reason and/or social justice. In doing so, the metanarratives defined ontological subjects as agents of history, recalling their identity, consciousness, and self-realization as immanent political actors. For example, in the real socialist metanarrative adapted from classic Marxism, the working class needed to recognize itself as an actor with inherent value, perception, and ideology to abandon alienation and steer the wheel of History through the siege of the means of economic production. The economic accumulation and the social inequality during the first industrial revolutions brought the metanarrative down to earth, in order to transform politics into a praxis to change the world. If history is a forward march, like a train moving faster in a path, the promise of a new world based on the correction of bigotry, obscurantism, and social injustice demanded to put the expectation in the final station called "utopia".

However, from the narratology point of view, this model would correspond with the classical myth of Icarus. This does not mean that utopias are always future dreams never reachable. Rather, the Icarus model of metanarrative resembles a historical process in which the brightness of the future silenced the importance of the becoming, the traveling action in the journey. As the mythological figure gained winds to reach the higher skies and fly for freedom, light and heat consumed the wings when he approached the sun. In the same allegory, the metanarratives above emphasized their teleological component while they ignored the becoming, the everyday modal philosophical part that connects the ontological departure to the teleological destination. In doing so, the historical events forgotten politics of the everyday, the tiny process of human life as actions of governmentality that are connected to exceptional futures and are as important to construct the promise of new humans in a continuous way. Rather, these metanarratives collapsed into autocratic regimes, rigid bureaucracies, inhuman assemblages of power, and quasi-total structures of surveillance for the sake of the actualization of the promise. That was the fate of the Icarus metanarrative model, either in Modernity programs based on rationalism and enlightenment or in socialist and equalitarian revolutions. It is not saying that their function, form, and content are fatally wrong. It means that the combination of their components in the metanarrative collapsed due to the emphasis on the ontological and teleological side of the quest, ignoring the modal or transformative part. Finally, if one can establish a slogan to this first

model, it is possible to utter: "We dream then we act". This is explained because the teleological promise functions like an engine that commands history and the political horizon of possibilities.

Figure 21: The Icarus metanarrative model



Source: the author

II. Sisyphus model

The second model represents the collapse of meta-narratives for resistance in the second part of the 20th century. Opposite to the previous Icarus model, this model only emphasizes the modal part: the becoming. It ignores the ontological and the teleological quest and oscillates eternally in the tension between no-actualization and no-political promise. The historical base of this model is explained by the technological, epistemological, and social changes in the political structure of the last century. Parallel to the expansion of technological networks, in the globalization of the economy, and the new order emerged after the Cold War, "master narratives" and "big" political projects became lousy, diffuse and fragmented. Moreover, the defeat of real socialism implied the end of big clashes between macro-political alternatives, and the crisis of macro-resistance projects as the world became dominated by a common economic matrix program.

As content of this model, one can mention the idea of rhizomes and networks in surveillance, in which the paths of resistance are implanted in labyrinths and kaleidoscopes. The loss of social orientation was shared with liberal agendas, anti-essentialist deconstructionism, post-structuralism, and some radical

analysis that abolished major teleological principles and meta-narratives since the 70s. Those trends have big differences. For example, one can cite the liberal idea of *End of History* by Fukuyama (1989), in which the world has reached the last historical step attained to liberal democracy and neoliberal economic agendas from Western countries. In this vision, alternatives to liberalism were futile and metanarratives of resistance lost their function. In other approaches, as in the *Liquid Modernity* of Bauman (2000), modernity became a flexible scheme of social relations and the political structures melted into modal forms of control and fluid dynamics of power. In parallel, Foucault's work can be summarized in the analysis of knowledge, power, and subjectivities to deconstruct those issues. He always admitted the possibility of resistance, but he also believed there is no major truth for politics, only relations of power that cut across subjectivity when someone becomes politically engaged (Foucault, (1984) 2019). Meanwhile, Derrida was the master of deconstruction. His *opening lines* refined the art of differentiation and introduced Copernican paradigms to analyze objects, bodies, and power. Those lines are opened by aesthetics and political subjects through the reconfiguration of language. Thanks to writers like him, we know that language matters, and therefore one should play creatively with it (Derrida, 1978). However, whereas Foucault's reaction to the loss of truth dilemma is to plunge into the free-for-all that remains, Derridas´s reaction is to retreat to an aesthetic haven of linguistic play (Stocker, 2006).

As other examples, *Our Broad Present* by Gumbrecht (2014) supports that the chronotope or "place of time" in present history is frozen and crystallized between idealized pasts and frightening futures. Moreover, in the *Society of the Spectacle* by Debord ((1967) 2012) and *Simulacra and simulation* by Baudrillard ((1981) 1994), those authors share the idea that time has no origins and ending due to the always-ongoing process of creating symbols, spectacles, and distractions that capture every sense of reality. In addition, based on the Derridian term *hauntology*, Fisher (2014) supports that the current generations are forsaken of future, of promises, and the only path is the becoming of what will never occur or that could have happened, directing a nostalgic gaze to past and present. Besides, the modal ontology worked by Agamben (2016) tries to overcome the Aristotelic division between the essence and existence of things to propose a new ontology based only on the modal processes of continuous becoming. Furthermore, in *The scent of time* by Han (2017), the present time has an increased predisposition to technical performance, auto-exploitation, and subordination of subjects rather than the thoughtful time to nourish ourselves. Even in the de-colonial post-Marxist approach of Spivak ((1988) 2016), she argues that there is no room to subaltern voices insofar as they are coopted by hegemonic voices and values that cannot be ignored in every subaltern reaction or process of emancipation. Thus, in different levels, the content elaborated by those authors exemplify the abolishment or the discredit of metanarratives. And even if some authors like Esposito (2013)

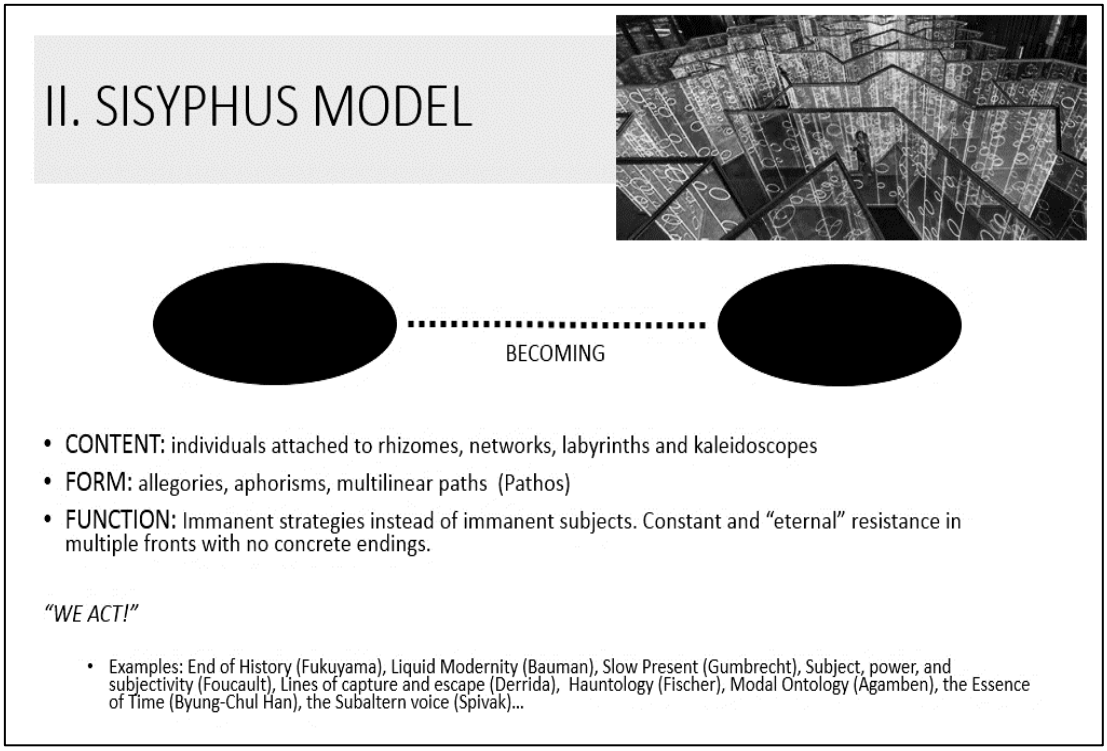
continued to explore concepts such as biopolitics beyond Foucault, he argues that either life appears as being captured as if imprisoned, by a power destined to reduce it to a simple biological matter, or else politics risks to be dissolved in the rhythm of a life that endlessly reproduces itself beyond the historical contradictions by which it is invested. In that sense, Esposito moves between pessimistic and optimistic accounts of life, depending on its relationship with apparatus of capture and circumscription (returning, somehow, to the above Foucault dilemma of resistance). Finally, drawing from the current Brazilian and Spanish context, Matos & Collado (2020) present the radical, common, inoperative, impersonal and fluid dimension of life that emerges from itself as inassimilable resistance, that is, as a bioemergency. Drawing from authors such as Simone Weil, Emanuele Coccia, Judith Butler and Nikolas Rose, in times of pandemic crisis, they affirm that the power of life arises in all its excesses and as a (dis)constitutive entity. It emerges in constant struggles against the micro/macro powers that seek to tame it. However, the authors disregard a phenomenological and normative dimension for this dispersion and force of life. Life transgresses norms and is always self-constituted as resistance. For them, life would not be able to be totally tamed. Yet, it seems that it cannot follow a major path or a metanarrative either.

Regarding the form of this model, most of those authors emphasize a sort of language based on allegories, aphorisms, multilinear paths, and pathos (emotions and feelings) as opposed to the forward linear and straight logocentric language to construct narratives. Regarding the function of this model, those examples describe immanent strategies of resistance rather than immanent subjects. It means that resistance is valued in terms of modulations, transformations, conservations, and transposal of tactics between actors, rather than identifying ultimate political actors (i.e., the idea of a fluid and ever-changing multitude against the unified and classic Marxist working class based on labor). For resistance, as there is no teleological point of arrival or sense of ulterior direction, this function implies a constant and "eternal" struggle in multiple fronts. In surveillance, we saw that the idea of "sousveillance" resembles the notion of constant and continuous resistance actions in different rhizomes of the surveillant assemblage with no clear endings. In surveillance, furthermore, Gary Marx (2009) proposed a cyclical sequence of neutralization (resistance), counter-neutralization, and counter-counter-neutralization (and so on). The sequence enlists a broader array of interconnected social actors and a dispute of technologies, tactics, and visibility/invisibility. Finally, even the four streams of resistance identified in Chapter 5 can be interpreted according to this model. There can be more interpretations, but, in this one, resistance would be converted into a set of multilinear and dispersed actions with no endings.

From the narratological perspective, utopias are erased from the horizon of politics insofar as this model can be labeled as the Sisyphus model. In Greek mythology, Sisyphus was a king punished by gods for his self-aggrandizing

craftiness and deceitfulness by being forced to roll an immense boulder up a hill only for it to roll down when it nears the top, repeating this action for eternity. In the same sense, resistance from the works above appears as a never-ending task conducted with no sense of teleological orientation. The authors above are exceeding skilled-craft men of political content and forms, yet, their 'grandiloquence' lacks a willingness for the 'promise'. We are conscious of the injustice and simplification of their work into a single archetype or model. Yet, for them, the resurrection of general narratives that explain the world would entail embracing the futility of finding universal paths to orient the collective agency. In doing so, every act of resistance is constantly repeated in a time that seems collapsed into the void of the eternal and slow present, a time without expectation of major historical ruptures, let alone the idea of future related to a universal 'redemption. Albert Camus, in his 1942 essay *The Myth of Sisyphus*, saw Sisyphus as personifying the absurdity of human life, but Camus concluded that "one must imagine Sisyphus happy" as "The struggle itself towards the heights is enough to fill a man's heart." In other words, everyday resistance actions and victories matter and must be recognized. However, the slogan of the Sisyphus model would only be "we act!", as the dreamy quest is extracted from the full potential to actualize a major promise beyond the resistance actions themselves.

Figure 22: The Sisyphus metanarrative model



Source: the author

III. Orphic model

The third model represents our attempt to reconstruct a metanarrative in the present time. In the face of the increasing instrumentarian power of surveillance (individuals becoming mere instruments) (Zuboff, 2019), the growing extinction of ecosystems, as well as the rampant socioeconomic inequality in most of the countries, the promises of linear progress that started in the turn of the last century seem to vanish. At the same time, the logic of social differentiation in surveillance (see Chapter 6) is increasing exponentially with particular outcomes. As in the field of astrophysics, where celestial bodies are tearing apart from each other, i.e. galaxies and stars accelerating in opposing directions in a process known as inflationary expansion of the universe, the socio-technical process of differentiation promoted by surveillance is deepening the process of differentiation of systems in politics. Despite the increasing scale of hyper-connectivity in terms of technical devices and the broader information available to users, one can express that there is even more disconnection between the social spheres. For example, the representatives appear detached from the people they supposed to represent in many countries, the technical/academic expertise tends to specialize and disconnect from the general people, social movements appear isolated from institutional grounds, the speculative economy in the accelerated globalization goes separated from productive and commercial activities, and the information between social groups follow patterns of echo-chambers or bubbles rather than fluid networks that connect actors, as seen in the last Chapter.

Hence, contrary to the last model, we propose the resurrection of a metanarrative that re-connects the differentiation of those social practices but keeping their inner differences and changing essence. It consists of connecting differences even if it sounds like an oxymoron. In that sense, a new meta-narrative project must encompass different social objects, being flexible and open to experimentation. Thus, we propose a metanarrative based on processes of becoming, leaving the door open to ontological quests of actualization.

Here, the departure point is recognizing that there is always room for transformation and mutability for people and social objects, and there are no ulterior/absolute ontological essences. In our "liquid" and fluid world, concrete essential ontology characteristics of subjects are eroded because of their mutable nature that turns impossible to formulate a stable and permanent definition of immanence (the question "who we are" cannot be answered permanently or absolutely). Even in the philosophy of science, there are forms of speculative metaphysics that privilege the events and processes above the substance with the consequence that we are released from the mechanistic, deterministic universe that is a product of classical physics (Peters & Besley, 2019). Therefore, we give importance to the becoming process or transformative action of things in

incremental or disruptive paces. In turn, this transformation seeks for teleological promises that orient the political action despite never-full endings. Thus, we speak of immanent strategies of resistance, rather than immanent subjects, as agents are mutable but their strategies and tactics acquire essence as they seek for new futures.

This is a negative ontology approach that, along with Adorno´s classic definition, rejects both the invariant ontology of transcendent being and the nominalist's denial of the existence of abstract objects. That is, the essence is found within appearances and interactions, not beyond them, and is understood in terms of difference and non-identity, rather than pure identity. In other terms, negative ontology interlinks existential and essential possibilities –not only strict actuality. By speaking in terms of "possibility", we mean that the ontological reading goes beyond determinism and contingency within it. In short, this is an open, not a closed, "reading of things". Hence, we can speak of a "negative ontology" or a never-completed ontology departure point that demands a thoroughgoing process (ever-going modality) trailed in concrete paths to navigate to teleological horizons.

In terms of content and concrete examples that would fill this model, we can mention the transcendent nihilism by Ray Brassier. To him, the teleological promise of history is death as he criticizes that philosophy has avoided embracing frankly this destination. In this path, individual subjects would never realize a meaningful ontology whereas they expect their annihilation (Brassier, 2008). In this content, surveillance would be the "pipe organ" playing while we go to extinction as species on Earth. Another yet distant example is Xenofeminism created by the Laboria Cuboniks collective in 2012. Like the pioneering *Cyborg Manifesto* by Donna Haraway in 1985, the goal of cyber-feminism was to propose a utopia to imagine a technological system dedicated to the emancipation of women and other marginal identities historically marked by difference (Hester, 2018). Yet, Xenofeminism (XF) uses alienation as a stimulus to generate new worlds. It flags the alien (the other, the strange, and the non-human) as a strategy to manage alienation (the worker turned into a commodity).

However, unlike Haraway, XF renounces the parody, irony, and performance that characterize postmodernism as rhetorical strategies and political methods to constitute itself as new rationalism. XF claims the orphan legacy of modernity, affirming that leaving reason or rationality (and technology) as patriarchal tools would be a tremendous error. At this point, Xenofeminism coincides with the *Manifesto for an Accelerationist Policy* signed by Nick Srnicek and Alex Williams. In this perspective, given the relative poverty of 'reasonable' contemporary political alternatives, the only radical political response to capitalism is to accelerate their uprooting, alienating, decoding, abstracting tendencies (Srnicek, 2013). In that sense, left-wing accelerationism maintains that precipitating the destructive dynamics of capitalism, instead of attenuating them,

means understanding that modernity is a transforming force and not a condemnation. In short, with important differences, both Xenofeminism and Accelerationism readapt the Icarus model from classic Marxism and appeal to the transformation or collapse of the system through a rationalist project to complete the promises of Modernity. XF, for example, strives for a globalist, anti-racist, anti-hierarchical, and transfeminism policy. On the other hand, right-wing Accelerationism theorists propose an active becoming that supports the intensification of capitalism itself, possibly in order to bring a technological singularity like Artificial Intelligence (AI) and post-human futures. Here, the existing infrastructure is not a capitalist stage to be smashed, but a springboard to be launched towards post-capitalism.

Prominent theorists include Nick Land and the works of "The Cybernetic Culture Research Unit" (CCRU) that intercrossed post-structuralism, cybernetics, science fiction, rave culture, and occult studies. In the germinal accelerationist matrix, "there is no distinction to be made between the destruction of capitalism and its intensification. The auto-destruction of capitalism is what capitalism is. "Creative destruction" is the whole of it, besides it, there is only retardations, partial compensations, or inhibitions (Land, 2017).

Finally, more theories from the previous metanarratives models have also been "updated" to this model. In a trend called "politics of subjectivities", thinkers such as Rancière (2011; 2015) and Rüsen (2005) support a negative ontology to rescue a bigger orientation to History. Guldi & Armitage (2014) also reaffirm the role of historians and intellectuals to speak truth to power so as to reestablish a "big" history to guide ethics, even if those professionals have different roles nowadays than fifty years ago. All the same, in this trend, politics also values the quest of new political communities based on the promise of dissent and humanism. We will attach our meta-narrative project to this latter trend.

In terms of form, those examples mix heterogeneous allegories, aphorisms, multilinear becoming, and forward-narratives in order to pursue "bigger" telos or destination. In an overall sense, those projects combine the "logos" and forward characteristics of the Icarus model, plus the "pathos" (emotional and sensible mutable dimension) and the ever-changing becoming characteristics of the Sisyphus model. However, in terms of function, those examples cannot be considered as metanarratives in the whole sense because they point to specific directions or promises that cannot be universalized. For example, XF circumscribes its actions to rationality and technology, as these can be a site of a dispute to anti-patriarchal approaches. Yet we think that those circumscriptions can be expanded adding connection points with other resistance projects. Macro projects of resistance might arise if current approaches and streams receive broader teleological directions to ulterior political endings. We do not aim to invalid the political quests for more legitimacy or abolish the epistemological development of

the previous examples. But, since many theories influence other ones, we want to create a narrative in which some of those examples can be recombined and integrated to enhance their potential, amplifying their impact on a larger scale. That is, we want to help some of their features proposing a metanarrative project, rescuing a "master" narrative to guide politics. To do this, we need to establish universal telos in which different projects can converge and detach to oscillate and promote big social transformations.

The first step to formulate a metanarrative is to think in the combination of reason (logos) and emotions (pathos). In that sense, we argue that there can be as much poetry in a book by Ovid as natural language processing in computer artificial neuronal networks. So, why are these worlds so far apart? Logos or rationality may be a poetic way of seeing the world, but it may fall into the illusion that spontaneous-thoughtless-slippery pathos is not necessary. Meanwhile, pathos is a reticular passion to see the world but it can decay in the oscillation of a whirlpool, ignoring that reason, in its verticality and linearity, can open new forms of understanding. Reason without pathos is lifeless *techné*, sterile and cold instrument, an algorithm with corrupted code, disinfected scalpel without patient. Pathos without reason is incomplete, it is music without chords, a sculpture without height and depth, dance without a body. Furthermore, rationality is not just logic and order. Pathos is not just chaos. Both are the threads that weave and unweave the sense of reality and temporality. The strictest order is as overwhelming as the heaviest disorder. It is like the attempt to reach the far stars and infinity, overcoming death and therefore life. On the other hand, the most chaotic disorder is as creepy as the severe order. Like a concert that doesn't end. A surface-less painting. Therefore, as important to understand the world (and surveillance) is computer coding as literature, algorithms and speech, econometrics and affections. For the two worlds to meet, logos do not have to give up intelligibility and pathos does not have to limit imagination. It is necessary to intertwine both worlds in each person or among as many people as possible. Even if they specialize in one of those fields.

To formulate a universal telos to a metanarrative, the next step is to consider the four streams of resistance identified in Chapter 5 and their overall claims. That is, we should listen to the goals and demands that the civic agency strategies formulate when they challenge surveillance and hegemonic actors. Again, formulating straight answers would be misleading because of the contingent and ever-changing nature of civic agency. Yet, we can formulate major-principles that would serve as fixed points in order to create a path for the streams of resistance. These principles should not be closed to experimentation and concrete practices, but they must indicate a common orientation.

In that sense, behind the "noise" of resistance, it is possible to suggest that the first ironic stream based on communication basically aims to calibrate the

narrative and aesthetical functionality for/to collective actors. This stream demands a new "partition" of the sensible world and political dissent, to use Rancière terms. It demands a communicative bargain between visions of the world, working within the idea of non-conformity to fixed schemes to alter the evolution of politics. The second deliberative stream based on cooperation and deliberation is the traditional struggle to define consent within a political community. It refers to the battle between contingent versus universal values that can be used by certain communities in order to cooperate, deliberate, or create groups based on legitimate consent (including technical interventions to respond to surveillance). The third agonistic stream based on the "necessary confrontation" would be equivalent to the struggles that awake equality and justice beyond the mere formation of political groups based on consent. Beyond the array of groups and political preferences, they promote the creation and repartition of social justice. Yet, some of the agonistic tactics might prefer to foster liberty and restore traditional authority. In any case, they go beyond the idea of permanent communities and are inserted in the battle of values, via supra channels (focused on the abstract idea of people or general will that arises above specific communities) or infra channels (focused on individuals and their freedoms instead of general people) for civic action. Finally, the fourth stream of despair based on high conflict would be equivalent to the struggle between those who want to enlarge communities versus those who want to preserve the initial political community. That means, beyond the necessary conflict, this stream reconfigures societies to enlarge the size and plurality of the political community. On the one hand, some people struggle to reach greater levels of "peopleness" and social justice. Whereas, on the other hand, some people want to preserve the traditional "meaning and identity" of the political community to reach greater levels of individual autonomy maintaining the levels of "peopleness". Therefore, in all the four streams one can see the attempts and struggles to alter the meanings and shapes of political communities to reach new horizons, even if things want to be preserved as in the Lampedusa effect (to change everything so to preserve them). Even conservative sides of the streams recognize the mutable characteristics of the multitude and know that they need to mobilize in order to preserve their positions. Thus, the four streams do not point automatically to progressive or conservative directions.

However, one still needs to formulate a telos to orient and direct the "noise" in the streams of resistance. To do this, it is useless to formulate universal contents and forms in the metanarrative. That means, due to the huge differences, preferences, and motivations of diverse political communities, the idea of a universal consensus and common action (adding all the groups into a bigger group) is wishful thinking. Yet, we can formulate a universal telos in terms of "function" to the metanarrative. It is possible to propose a common function to suggest a path rather than impose a solution in this impasse. Thus, the telos must

be porous in order to be worked in the four streams (form discourses to conflict) and attached to the array of heterogeneous practices and changes of the multitude. As in classical metanarratives, it cannot be something concrete or material. It must be an intangible idea that is worthy to be pursued despite its never full accomplishment. And considering the "noises" of resistance, from aesthetic functions to the preservation/enlargement of a community", what is behind the noise of the noise is the re-elaboration and struggle to configure the repartition of political Legitimacy and the very idea of Humanity. In that sense, the metanarrative is a bi-dimensional path to rescue and bargain Legitimacy and Humanity. These principles should be considered as the telos behind the streams of resistance.

Let us explain these teleological and functional principles.

Legitimacy means horizontality and equality. This metanarrative keeps those directions from the Icarus model as it reconsiders all those practices that aim to create equality and horizontality. Citizens can have equal rights and duties either by jurisprudence or nature, but the lack of more horizontal conditions to balance those rights and the material relations between them eventually would undermine the very idea of equality. Thus, Legitimacy also means to reduce the material distance and opportunities between those who govern and the governed; refraining the power from those who decide governmentality tools, the regulation of flows of information, and the concentration of great authority in a few actors or groups. Horizontality does not mean the inexistence of social stratification at all and the abolishment of chiefs and leaders. Teachers and students, General and soldiers, parents and siblings, all of these contexts entail asymmetric notions of power and authority. However, horizontality means that power relations are built upon legitimate sources in order to refrain abuses, instrumental use of commands, and automatic rule. Indeed, even soldiers should have a voice and turn their Generals accountable by direct forms because they are intrinsically equals. As Rancière affirms, "There is order in society because some people command and others obey, but in order to obey and order at least two things are required: you must understand the order and you must understand that you must obey it. And to do that, you must already be the equal of the person who is ordering you. It is equality that gnaws away at any natural order. [...] Ultimately, inequality is only possible because of equality." (1999, p. 37). Thus, command and obedience are to be recalibrated even in hierarchical organizations. This implies empowering lower ranks in vertical organizations. No man and woman should go to battle just by following superior orders. Obedience should be triangulated according to its content as following orders without critical thinking could also lead to commit crimes (Milgram, 1974).

Equality also implies connecting realism in politics to moral and aesthetic dimensions, counteracting the notion that human nature is per se evil or that only

the strongest leaders are able to abolish chaos in an insecure world. Politics is a world of eternal competition but also of cooperation, of ruling and being ruled. Not all traditions are negative, and even obedience and companionship have a value in many cultures like in several Asian countries. Hence, an authority could be sustained by obedience, but obedience in turn must be based on legitimation. No person, party, and a group can congregate all the advantages of authority and legitimacy. The latter is enhanced by consequentialist approaches (as a goal) but especially by the substantive incorporation of dissonant voices (as a means). Thus, legitimation is harder to be achieved. Indeed, in times of crisis and insecurity, illegitimate scapegoats proliferate while strong and auto-referential authorities appear as "easy solutions" to solve social problems. In times of uncertainty, current psychological studies conclude that people might fear authority but paradoxically they can support authoritarian leaders and, at the same, they think they can protect themselves against authoritarian backfires (Petersen & Laustsen, 2020). However, politics is a multidimensional system (from logical to symbolic and heuristic dimensions) mobilized by an array of actors. Politics is not only a rational game of forces. Thus, the determination to concentrate all the authority and legitimacy in a single actor to fix society like an engineer is quixotic and dangerous.

Ultimately, equality means that the rulers and the ruled people have equivalent premises as subjects of actions and possibilities. It does not mean to erase all personal differences. Individuals are equal in their individuality. Equality is the promotion of equivalent notions of agency (potential action) and normative possibilities between individuals as no authority sustains itself (as an auto-referential object) for a long time, and authority should not be the ultimate goal of human action. For example, good teachers use their commands so as their students can learn and build knowledge. Generals should be accountable to their soldiers, and their actions must be the last resource to solve the tensions of peace. Parents ought to care for their children in order to foster as much autonomy and responsibility they can in their offspring, even in hard conditions.

Naturally, the difference of power in microsocial domains are easy to be represented in close groups as they enhance an authority based on prestige, expertise, and even tradition. However, since traditions are also mutable, the notions of authority that sustain any social relationship are harder to be represented in macrosocial domains and between distant groups. In macrosocial domains attached to distant groups, tradition is not enough to legitimate asymmetries based on nationality, sex, race, class, gender, education, labor, accessibility, biology, etc. as those dimensions overlap and are always dynamic. Thus, horizontality means to go beyond any notion of equality based only on subjects of rights and duties. It also means to erode illegitimate sources of power that sustain injustice, exclusion, misrepresentation, violence, and subtle abuse between distant groups – either by direct human actions or by the mediation of automated tools. In short, whereas equality refers to the rights and duties of

individuals, horizontality refers to power between social groups. Thus, equality intertwines but is different from horizontality. Even racial segregation enhanced by the Jim Crow Laws in the USA and by the Nuremberg Laws in Nazi Germany appealed to a strict definition of equality, preserving each one position in society and the "natural" distance of racial groups.

In that sense, equality is based on reasonability and individuality. Meanwhile, horizontality is based on notions of personal and collective justice between distant social groups. Therefore, equality and horizontality can have a connection but their relationship is not always harmonic. Their promotion also involves tensions as some groups struggle to achieve and transcend equality more than others, and some of them even act to block it.

In light of the above, if we consider Legitimacy as a teleological principle comprised of equality and horizontality, this principle aims to reduce the asymmetry between "powerful and powerless" people, or between watchers and watched in the case of surveillance. Even if absolute horizontality would never exist, Legitimacy fosters the synchronization between those who enact political decisions and those who follow them. The purest legitimate version in a political community would be the scenario in which the own *principals* or people decide upon their living conditions, reducing and ultimately eliminating the convergence of authority towards a single actor. It does not mean to abolish power but to redirect it. It oscillates from the intermediated concession of authority to the self-promotion of authority. This would be an experience in which there is room for prestige and leadership, but also to amplify the autonomy of subjects in a horizontal ground opened to cooperation and dissent, contradictions and coherence, rules and improvisation, routinization and contingency. Yet, we recognize that this ideal form of legitimacy is more like a telos worthy of trying even if is a destination never reachable. Perfect legitimacy in politics might be hard to be actualized, but its anarchic characteristic (in the sense of *an-arché*, no fated by a single origin, instead of unlimited liberty and permanent disorder) can reestablish the wheel of History and its forward movement to new political communities. In light of that, the purest form of Legitimacy channelizes equality and horizontality to fulfill any political action. It conceives the actors from the multitude as the receivers of authority (*potestas* + *auctoritas*) and not only as the authorization source or the base to legitimate stronger actors.

The purest form of Legitimacy should be pointed as a telos because the metanarrative interplays with ideal destinations rather than concrete and permanent destinations. Ideal Legitimacy as a telos should be directed according to the current conditions of hegemony and instrumentarian tools deployed on people in every political domain. That means, the greater the conditions to expand the asymmetries between watchers and watched (i.e. to increase the commodification of subjects, to accelerate inequality through implicit and explicit

domination of people, etc.), the more we need to put a telos in a distant destination to counteract and even neutralize those trends. A telos cannot be reformist, neither attached only to the creation of concrete institutions and forms of government (of course these aspects matter). Its pure form and condition should serve to redirect the path of resistance and the path of History, reestablishing a capital letter at the beginning of this word.

In that effort, the telos is bi-dimensional as it also refers to Humanity. Rather than a cultural-centered concept based only on material progress and on the westernization process that erases other differences through the conquest of spaces (physical, ecological, and virtual), Humanity should encompass the differences between cultures, as well as the hybridisms and the attempts to conserve, merge, and create traditions. Humanity here means incorporating a repartition of sensibilities, rationality, and alterity that interplay dynamically with social groups and nature. Humanity means recognizing individuals (and their autonomy) and the right to optimize their freedom in the encounter with other ones. It implies recognizing the other in us, and we in the other. It is the last wager to save humans, not as biological species, but to save ourselves as active subjects that readapt imperfections from reminiscent humanist traditions (Todorov, 2009). The other could be something or someone strange or impossible to understand. The other appears in terms of nationality, ethnicity, gender, sex, class, religion, age, access, education, and so on. The more the civic and collective actions enable a transition between those terms -as well as a comprehensive understanding of the differences and commonalities for the sake of autonomy and human presence (Gumbrecht, 2004)-, the more social conditions are being created to produce Humanity.

Humanity, thus, means to interplay with the gaps in the sensible dimension in everyday politics. The clashes and inevitable collisions between us keep us apart even if we belong to the same species. The bridge of alterity seems to be broken most of the time. Yet, if those gaps and differences constitute the very idea of Humanity, they also can be transposed. The ability to alterity is closely related to the human ability to discern different points of view including ours. It means obtaining the greatest panoramic view of beings and things, seeing our interdependence on the whole landscape. It entails an expanded way of thinking called *Phronesis*, the maximum political virtue for thinkers like Aristotle; the ability to think from others' positions. In this, if the sensible dimension of beauty, love, kindness, and alterity are forgotten in everyday politics, then disgusting politics would emerge as governmentality patterns difficult to be counter-balanced. Moreover, the lack of beautiful politics eventually would compromise authentic self-realization, from autonomy to personal liberty. This self-realization depends on the collective dimensions of Legitimacy as well as in the relationship with nature. Indeed, the more we deplete the ecological systems (some actors are more responsible by the ecocide than other ones and the rhetoric of humanity versus

nature is misleading), the more we confront ourselves within the same species, as (im)possible agents of alterity, and as (co)creators of destruction.

In that sense, it is also important to remind that this political virtue depends entirely on the horizontality of people's conditions. A thing can only be represented under multiple aspects when many people represent different perspectives. Its achievement is impossible in a reality where the “other”, as well as alternative views, is suppressed as in the case of tyrannies. Yet, in an informational world where everyone has a voice, before making judgments, being open to more people also works as a means for making better judgments, and assuming responsibilities for the “other”. In ulterior consequences, being isolated as well as suppressing and ignoring the “other” implies the lack of individual freedom and autonomy, as stated by Levinas. Thus, those ideas converge on Legitimacy and Humanity. These macro-principles depend on each other. They point out an ulterior path that must be attached to every social decision. Their union sustains the metanarrative because they can encompass everything. It is a master narrative in functional terms because it can be opened and triangulated with concrete beliefs around the world and with the streams of resistance in order to redirect and move again the path of History.

It is too dangerous to formulate a unique principle or unifying both terms (Legitimacy and Humanity) insofar as there must be a tension between them to boost social change and to be attached to resistance actions. Moreover, as the becoming or the modal part of the metanarrative is as important as the destination, the tension to promote Legitimacy and Humanity should be triangulated with everyday political procedures of transformation.

In doing so, the differences and conflicts among resistance groups do not disappear. Yet, they can find a common functional orientation instead of universal content and form. Both Legitimacy and Humanity would support every tiny action, strategy, and operation of resistance. Something comparable to robotic engines attached to molecules in biobots that spread in one ecosystem with no common form but with similar functioning. Other examples are energetic compartments like the mitochondria, which is a common function to living cells even in different tissues, organisms, and species. In that sense, the different strategies of the civic agency can be commonly boosted and oriented by Legitimacy and Humanity.

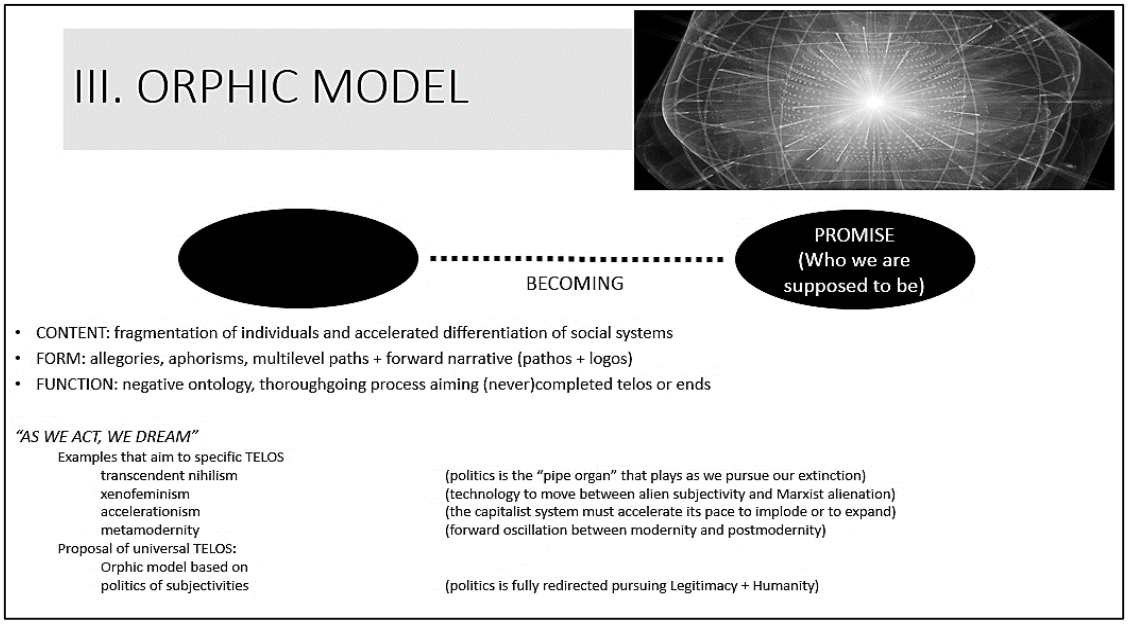
However, in this effort, we must learn from other epistemologies that evolved and share logic both from the Icarus and Sisyphus models. For example, post-Marxist and intersectional feminism have inherited a set of comprehensive theories that have points of intersection with this metanarrative as those consider gender, nationality, class, and ethnicity to analyze resistance and promote equality. In the end, they can point out to the same direction and can be better connected. They also have connection points via Legitimacy and Humanity. Of course, those

programs present differences in terms of content and form. Yet, rather than erasing their differences, some features of those projects can be boosted through a metanarrative that allows them to be reinforced with additional resistance forms, either in terms of epistemology or especially by the triangulation with the above principles. This is not merging proxy theories or adding all resistance forces in the world to produce a final synthesis. That would be wishful thinking. Rather, in our vision, different actors and beliefs can be incorporated and detached from this open model because of its negative ontology. Likewise molecules joining and detaching to produce molar patterns, what would keep different actors in constant communication is their commitment to sharing the same functional endings even if they do not share the point of departure or the becoming. Besides, not all epistemologies and resistance projects seek for the same teleological principles that we proposed. Thus, the functional telos is the base that eventually would help to communicate differences. It is a porous and tempered universal bridge to follow feasible actions and distant dreams. "Adversaries" or foes to Legitimacy and Humanity would add difficulties to pursue the metanarrative, but they will become actors to act against and objectives to be counter-acted. Those "adversaries" will constitute the "otherness" pole that keeps the alterity tension alive within different political communities, boosting social changes, and generating new scenarios.

From the Icarus and Sisyphus models, we also need to learn from the experiences in trauma, violence, conflict, and pain. The zones of silence, from past events in history to dark human motivations being reproduced in the present, are as part of our becoming as the beautiful and good parts of us (Rüsen, 2005). In other words, Humanity means incorporating confrontation and absurdity as they are also part of the becoming. This incorporation consists of not replicating mechanically zones of silence but understanding that the teleological path also encompasses zones of abysms and failures. History is not the teacher of life lessons (*Historia magistra vitae est*). In the classical form, History demanded that "we need to learn from the mistakes from the past". However, history never repeats itself but it resembles past situations that are similar yet unfamiliar. History comprises the broad zone between experience and expectations, between the past of the future and the future of the past (Koselleck, 2004). In light of that, History leaves its descriptive characteristic and becomes an activity of reflection and practical use (White, 2014). It supplies meaning to re-emerge from the abysms and allows to create memories and past uses that endure fallings, one after the other, like in the Sisyphus myth in which the figure continuously pushes up the rock to the top of the mountain. For example, thousands of people died supporting or fighting against the Icarus or Epic metanarrative model in the last century, including in Spain and Brazil. Thus, more than a sacrifice, that action of dying and living have something to tell to the new generations. More than historical facts and descriptive lessons, those actions redefine values and sensibilities and allow reflection to navigate in prospective times.

In light of the above, as our metanarrative share elements both from the Icarus and Sisyphus models, incorporating new ones, we can call it the *Orphic model* or *Orphic metanarrative*. For ancient Greeks, Orpheus was the figure that unveiled sensibilities but also rational awareness. He enchanted creatures with his music but, like Sisyphus, he went to the underworld and was punished by the gods losing a beloved person. Yet, despite the zone of silence in the heart (the traumatic past events of History), Orpheus became a founder and prophet of the so-called "Orphic" mysteries. He was credited with the composition of hymns and shrines containing purported relics that were regarded as oracles, sacred sites of arts and science. Even during war and peace, the oracles were the fixed path to consult and to listen during easy and hard moments during the Antiquity. Orpheus was dead by those who did not hear his music. In that sense, the Orphic metanarrative needs to struggle against those who cannot hear Legitimacy and Humanity. The Orphic model is not only a story of self-recovering and empowerment. Its motto is "as we dream, we act". It is similar to Metamodernism, a proposed set of developments in philosophy, aesthetics, and culture that mediates aspects of both modernism and postmodernism (Turner, 2011; Van den Akker, Gibbons, & Vermeulen, 2017). Yet, Metamodernism establishes an oscillation as the main form to overcome the disenchantment of modernism and the labyrinths from postmodernism. Likewise, our proposal also oscillates between the Icarus and Sysiphus models and aims to go forward. Also, more than going forward, the Orphic model establishes a universal teleological path. This path consists of pursuing Legitimacy, equality and horizontality, and Humanity, individual autonomy and the dynamic connection between the threads and gaps of rationality-sensibility, even if these destinations are not fully reachable. It consists of a teleological quest of beautiful politics despite many obstacles and uncontrollable disgusting politics.

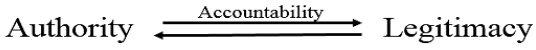
Figure 23: The Orphic metanarrative model



Source: the author

The desert is advancing: Accountability revisited

So far, we have understood accountability mechanisms as connectors between authority and legitimacy. Either by procedural steps or by a consequential approach, authority, the capability to execute and deploy a public decision, relates to a base of legitimacy. Meanwhile, legitimacy is not an auto-referential process. Legitimacy gains amplitude and scope when connected to an authority that accomplishes it. In the political realm (from institutions to radical civic agency), we mentioned that legitimacy without authority is an "empty" power. In that sense, in the theoretical framework, we postulated that accountability establishes a dialogical connection between authority and legitimacy. When a player "A" is called to account before a player "B", there is a relationship that looks for justification or correction of outcomes regarding the execution of a certain policy. In public accountability, authority is called to legitimatize their actions. As observed in the figure below, accountability core meaning is activated to build a connection to replenish authority and legitimacy.



However, if we consider the Orphic metanarrative model, the transformations of politics guided by the bi-dimensional path of Legitimacy and Humanity, it is important to combine both telos in a process called triangulation. That is, Legitimacy and Humanity poles (LegHum) need to be attached to third concrete practices, as molecules connect and bond to new ones to formulate new substances. In that sense, LegHum can join concrete accountable practices in order to tackle authority. In surveillance, when authority is an embodying form based on hegemonic instrumentarian power (i.e. executing the pathological side of surveillance over data subjects), then the triangulation between the ideal telos "LegHum" and concrete practices of accountability can redefine the core nature of authority producing a new substance: politics based on agency. The agency level refers to the ever-changing power from the multitude that encompasses civic actions based on dissent and cooperation. Contrary to the hegemonic or top-down "lines of capture" embodied by the authority, the ideal new substance will represent bottom-up "lines of escape" in political actions, as follows:

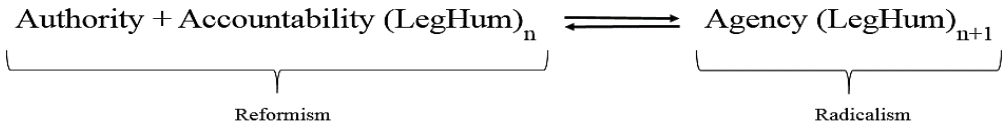


Table 21: Political "equation" to restrain authority and generate agency

Authority	Embodying a form of power based on hegemonic or instrumentarian power (top-down lines of capture)	
Accountability	Reformism Principles to restrain the authority: Responsibility Transparency Answerability Enforcement	Radical Principles to generate agency: Representation Consultation Participation "Presentation"
Legitimacy	Based on: Equality Horizontality	
Humanity	Based on: Autonomy-alterity Rationality-Sensibility	
Agency	Ever-changing power from the multitude based on dissent and cooperation (bottom-up lines of escape)	

Source: author

The figure means that authority can react with the triangulation between accountability and LegHum. In that sense, authority is restrained and redirected to produce a new political substance: agency. The left side of the equation is the part of reformism insofar as accountability is based on a set of values (such as responsibility, transparency, answerability, and enforcement) that redirect authority but do not "break it" into a new substance or change its nature (a constant source of production of lines of capture). Authority here constitutes the main object that reacts with the triangulation Accountability-Legitimacy-Humanity, in a continuous process repeated "*n*" times. This is because accountability is triangulated with the teleological search based on Legitimacy (based on subjects' intrinsic equality and horizontal power relations) and Humanity (individual autonomy and alterity between social groups and nature, and rationality-sensibility) through an ongoing process of becoming. In that sense, the triangulation should be executed continuously from exceptionality to governmentality, from high-politics to everyday politics.

On the right side of the equation, a new substance is produced: politics based on the triangulation between LegHum and agency (the ever-changing multitude based on dissent and cooperation). This side represents the ideal form of politics based on "lines of escape" repeated "n+1" times. Contrary to the Deleuzian "n-1" concept that cancels totality subtracting one element to the unity,

implying in impossible unification in terms of resistance and agency, here "n+1" means that every molecule of authority is broken in at least "+1" molecule of agency, it represents the unity broken into more pieces of the multitude. "n+1" also represents the times that the triangulation between the agency and LegHum must be conducted. In the reformist side of the equation, the triangulation with accountability is a continuous task from exceptionality to governmentality. On the other side of the equation, the triangulation with the agency must be conducted always in a completer intensity and degree when compared to the one related to authority. Agency self-governed by the telos of Legitimacy and Humanity is harder to be produced and must be conducted always in a more meticulous and precise manner; thus, it must be conducted "n+1" times. "n+1" is the radical dimension of politics insofar authority and accountability lead to a new substance or form of politics based on continuous lines of escape being produced in ever-changing becoming processes based on the negative immanent ontology of subjects from the multitude. It is the radical or pure form of self-governance, autonomy, and horizontality. It has anarchic characteristics (in the sense of an-arché, not fated by one single origin or past, rather than chaotic disorder) and is the pure and ideal stage of politics that converts authority into pure agency.

Finally, the arrows in the equation mean the transition between the two sides, from reformism based on lines of capture to radical politics based on lines of escape. As history is not linear and politics is not homogeneous, it is possible to find both stages at the same time in the social reality. That means, in a certain society, there are niches where is possible to find the reformism side, for example, in institutional and legal attempts to restrain authority (as in the case of internal and external controls of intelligence agencies exhibited in Chapter 3). At the same time, some niches are related to the second radical side, for example, in the strategies and tactics formulated to challenge surveillance by the multitude (as in the case of some streams of resistance identified in Chapter 5). Yet, both sides of the equation are in continuous tension implying in a bidirectional interaction (double arrows). There are no pure forms and examples of each side of the equation, as lines of escape always interact with lines of capture and vice versa. Because of the negative ontology, not every form of authority is illegitimate nor is the agency purely legitimate. However, by pursuing the bi-dimensional telos (LegHum) and its triangulation with concrete actions of accountability, the ideal orientation would try to reach greater levels of the radical side in the equation. That is, considering the asymmetry of power between the lines of capture and the lines of escape, it is evident that we need to search and promote the latter ones in the agency/multitude to restrain and reduce that asymmetry. Not only is necessary to turn every form of authority more legitimate, but it is also essential to promote greater levels of LegHum in the agency to counteract the lines of capture from authority. Radicalism means an action that tackles the roots, the main base, and the core of authority. It represents the main goal of accountable politics intersected by

Legitimacy and Humanity. Instead of radicalization, a banalization of the word "radical", as in the realm of security and antiterrorism, to be radical means that it is necessary to aim radical telos, radical becoming, and a radical metanarrative if we want to leave behind the Sisyphus and Icarus models of political action. In that sense, we will be able to reestablish the wheel of History and its forward movement to new political communities at local, national, and international levels.

In that logic, when contrasted to our concrete case studies, how the new equation of accountability can be exemplified? How the triangulation between Legitimacy, Humanity, and real accountability practices can be executed?

Considering the first realm of this study, surveillance in intelligence, accountability can be promoted in the reformist side as attested in the previous chapters. That is, by deepening and strengthening the mentioned accountability principles: responsibility, transparency, answerability, and enforcement. In that sense, responsibility consists of strengthening the internal controls, audits, administrative/economic mandates, and professionalization from intelligence services in order to promote liable actions and policies. Transparency relates to the "deferred visibility", a form of disclosing certain information from operations, capacities, logistics, and actions of intelligence, but preserving the sources and actors that conduct those operations. As seen in the first part of the study, this principle is especially promoted by the role of media and civil society. In turn, those can spark further mechanisms such as legislative and judicial controls, as well as international accountability networks. Answerability, the capacity to demand answers, justifications, and explanations (a priori or after wrongdoing), is enhanced especially via institutional controls, but it also should be fostered by informal mechanisms played by scholars, media, pop culture, and the civil society. Lastly, enforcement should be improved in legislative and judicial controls in order to keep intelligence services in the zone of legality. This principle also helps to monitor the suspension and the preservation of rights and liberties from citizens, including those groups considered as threats or foes to the establishment. In that sense, the role of judicial bodies is essential and we recommend the creation of this kind of control in the Brazilian case (see judicial control in Chapter 3).

Notwithstanding, the above forms of accountability are mainly formulated to tackle intelligence through actions that flow into the direction of the authorities elected by the citizens (representatives that control intelligence services), rather than to the population itself. However, intelligence services that wish to increase real legitimacy would be more porous to citizen agency and would point out to the second part of the equation in its radical form. In other words, accountability needs to be added with further principles that pave the road to even greater legitimacy scenarios. To reach them, other accountability values need to be developed: representation, consultation, participation, and "presentation" (continuous presence and participation) as expressed in the last table 21.

Representation means the classical mode of agents and principals that allow (authorize) authorities (politicians and policy-makers) to delegate mandates and rules upon specialized bureaucracies/institutions to conduct governmentality actions. In that sense, citizens elect representatives and confer them with authority (first degree of legitimacy), in turn, the authority indicates the chief of staff that commands the intelligence bureaucracy. The flow of this kind of representation is unidirectional insofar as intelligence chiefs and professionals do not report directly to the citizens, rather, they report to the representatives/authorities in the three branches of government.

In addition, consultation means that besides the representation form of accountability, intelligence and other bureaucracies can report to certain citizens in order to endorse internal decisions and political outcomes. It means a policy conducted mainly by internal and specific criteria of the bureaucracy and eventually by encompassing citizens' preferences to obtain the consent and implicit support to already-taken decisions.

On the other hand, participation means substantial incorporation of co-decision-makers in the policy process and in internal bureaucratic mechanisms to control intelligence services. It goes beyond the mere consultation and communication with citizens, in order to integrate them in the very process of decision-making, increasing the levels of accountability and legitimacy to astonishing levels. As intelligence and other bureaucracies work under secrecy and dissuasion, the participation of citizens in the formulation and control of policies would require to create restricted participant groups from the population in order to build audiences, chambers, and committees pointed by institutional channels but also chosen randomly from the citizenry. Those audiences would need to obtain security credentials, have temporal mandates to execute their actions, and their backgrounds should not affect the security of intelligence operations. Preferably (but not compulsorily), they should have expertise or knowledge in external controls and accountable actions, from ethics to economics. Those groups would need to gain power before other commissions (from parliaments and representatives) or participate with them side by side, in order to evaluate outcomes and prospective intelligence policies. At the same time, those groups would need to gain access to judicial authorization reports on a regular base to verify their consistency and lawfulness, having the capacity to appeal to the Supreme Court in case of wrongdoing and misconduct of judicial oversight bodies. In that sense, the groups would go beyond the mere consultation principle and the ombudsman role to protect guarantees and fundamental rights. These groups would need to participate alongside legislative and judicial controls, having the ability to access classified materials and evaluate intelligence operations with almost no restrictions. In doing so, they will need to elaborate two kinds of reports: one public/open report released in a regular base, with deferred transparency measures; and a second one with restricted and classified content that will only be

disclosed after a certain time, indicating details and operations from authorities and intelligence members. That means to reinforce declassification standards and access to information policies in accordance with disclosing rules of national security in each country, contributing to the legitimacy of intelligence even in a posteriori form (following different terms of declassification according to the sensitivity of the protected materials and information).

Finally, the "presentation" principle of radical accountability consists of direct continuous presence and participation. When applied to intelligence arenas, it would consist of reporting especially to a commission of citizens chosen randomly by the above-mentioned criteria. That means, instead of reporting especially to representatives of the people (representation), intelligence would report mainly to a chosen group of citizens (including people from different backgrounds and formation) in order to discuss, elaborate and evaluate intelligence and national security policies. This communication would be official and located above the links with parliaments, courts, and institutional groups. In emergency situations, the formulation of policies would be communicated and formulated with three members of the commission that in turn will authorize and share forthcoming outcomes from intelligence with other members. The commission or group will work alongside Supreme Courts and judicial bodies. In that scenario, the parliament will be chosen following the same criteria of the commission, meaning a new form of elections based on specific terms, and random criteria as in the case of the principle of participation. Finally, this scenario means the substitution of the partisan-executive representation system by a network of commissions distributed alongside different policy arenas that oversee bureaucracy, ministers, and the administration (AsimAkopoulos, 2016). This scenario enables greater institutionalization levels of the radical side of the equation. As this scenario is ideal, reformative approaches should enhance the proliferation (incremental or disruptive) of the radical accountability principles, allowing at least experiences of consultation and participation, and, in the best scenario, allowing experiences of "presentation" (direct continuous presence and participation). Intelligence might be exceptional in the implementation and operations but not in its construction and assessment. Thus, it can be overseen closely by the citizens.

The best scenario would need to cope with current and prospective problems affecting entire populations, such as the technological developments related to mass surveillance. In that case, and considering the bulk data collection aims to prevent attacks and threats, rather than decreasing surveillance, it would be better to increase transparency as greater exposure eventually can enhance accountability. Even though there is no clear evidence that mass collection has avoided any unwanted action, only banning or waiting for clear indications of threats might have counterproductive consequences. The problem is not surveillance per se, but the violation of privacy, the unchecked categorization, and

matching of data to profile (purposes), as well as the intrusive, disproportional, and scale (means) that might be fostered by surveillance. As each purpose and means has different scopes, it is misleading to forbid every collection and use of data. The solution, therefore, would be to address accountable actions in each of those purposes and means as proposed in the realm of personal data in this study.

*

In the second realm, we have shown accountable actions regarding the governance of personal data. Here, accountability principles such as responsibility, answerability, and enforcement were enhanced by the regulations to protect personal data. The new legal frameworks added porous guidelines stemmed from market practices, such as Privacy by Design. However, those regulations need to be expanded on the international scale and reinforced by demanding embedded privacy solutions in the designs of devices, services, and manufacturing of technologies that process personal data. This would limit mass surveillance abuses and enable universal privacy standards that cannot be turned off by those in power (HTTPS connections, encrypted VoIP, Host-Proof hosting, and Anonymous Credentials are examples of technologies that can be implemented in devices and services since the moment of their creation). Moreover, accountability has to be enacted at a global level, both to governments and industry and in every different sector of society (Monteiro, 2014). However, technological solutions are not sufficient and cannot be regarded as overall solutions in the governance of personal data. In the market domain, we have shown the importance of transparency and answerability to correct the use of data in technical issues such as algorithms and the link between giant data processors and governments.

Notwithstanding, the above forms of accountability are formulated in the interaction between official authorities and market data processors, and they focus on strategies to control, process, use, and store personal data. The weaker side of the equation, the civic agency strategies, thus, was addressed to complement and awake new forms of governance, even by resistance and conflict. In that sense, data regulators and processors from states and markets would need to be porous to citizen agency demands related to the second part of the equation in its radical form. In other words, accountability would need to be added with further principles that pave the road to greater legitimate levels in the governance of personal data. As mentioned above, those principles are representation, consultation, participation, and “presentation”.

In this realm, representation means that data regulators (legislators and data protection agencies) act in the name of users and principals (citizens) to enhance their rights. Consultation means the users' opportunity to defend data rights such as access, rectification, cancellation, opposition, and portability across distinct data processors. Here, individuals have a leeway to interact as agency

subjects to correct or challenge the use and content related to their data. In the case of market organizations, representation means that data processors flag the best interests, preferences, and offer services according to their customers. Yet, as intelligence services report mainly to elected authorities, market processors report mainly to shareholders. Thus, if we want to move forward to more radical accountability actions. We need to address consultation, participation, and "presentation" principles.

Consultation in market practices means to adopt privacy by design, to ensure users demands and needs, and to create user-centered platforms to offer goods and services. If companies want to create trust with customers, they should consult their interests and preferences. Indeed, companies such as giant tech processors are efficient to offer personalized services. However, they do this via instrumentarian patterns that promote the commodification of users' data, thus, neglecting Legitimacy and Humanity ends. To change those patterns, market organizations should change radically their form of doing business, being porous to participation and "presentation" accountability principles. This leads to a revolution in the very way of capitalist practices attached to market organizations nowadays. In other words, it is necessary to think in further ways to turn markets more accountable, beyond the interest of shareholders and owners, and the monetary profits and benefits extracted from their services.

In 1992, the American writer Francis Fukuyama proposed that history was dead and capitalism was the only survivor. Margaret Thatcher had already warned before "there was no alternative" to the free market. Furthermore, the philosopher Mark Fisher and his concept of "capitalist realism" already warned about the metanarrative characteristic of this system that everything coopts and encompasses. Indeed, the late capitalism functioned as a quasi-metanarrative in which the entrepreneur spirit and the desire of individual satisfaction converged (Dardot & Laval, 2014). It mobilized principles such as enterprise, liberty, and even security remaining as the last macro system of thought and action. However, the accelerated capitalism of the recent five decades based on market deregulations is far from being perfect. Although a profound change of this system may sound as fictional as traveling through space-time, a wind of change blows in the air. A specter is haunting Europe (and the world). Due to the array of contradictions[145] caused by the phagocytosis of societies to economic powers, "men should not be

[145] Over the past decades, millions of people have seen that they have work, but it is insufficient to lead a decent life; that the social elevator has slowed down; that inequality is immense in the planet; that greed seems the most conjugated verb for finances and that the climate crisis could reap a future for their children and grandchildren scorched with ashes from the ecocide (Higgins, Short, & South, 2013). In addition, the world changed from a financial economy, where parameters determined the value of companies, to an economy of intangibles. 85% of the capitalization of S & P500 companies comes from intangible assets and only 15% of financial assets, just the opposite of 40 years ago. In: Ross, J. 2020, February 11. 'Intangible Assets: A Hidden but Crucial Driver of Company Value'. *Visual Capitalist*. Retrieved from https://www.visualcapitalist.com/intangible-assets-driver-company-value/ in 03/02/2020.

governed by any authority they cannot control."[146] Moreover, "We live in the time of capitalism. Its power seems inescapable. But so did the divine right of kings", as expressed by the poet Ursula Le Guin in 2014.

Even top CEOs and economic elites from giant tech processors are conscious that eternal growth is impossible. Business based on short-term benefits, and excessive economic competition overriding social and environmental outcomes needs reformulation. For example, in 2018, a report of top industrial and financial companies called the Business Roundtable (BRT), one of the main American business forums that integrate 181 large organizations including giant-tech data processors, released a report to redefine the "purpose of companies". According to the report, shareholder earnings are as important as protecting the environment and promoting diversity, inclusion, dignity, and respect. In that sense, the business needs to create value for all stakeholders.[147] In addition, a list of 25 large companies that include technology giants has reacted against the US withdrawal from the Paris Environment Agreement. The companies support international actions as the only way to avoid the "ecological disaster". [148] Even the conservative British newspaper Financial Times embraced the movement in September of 2019 shocking its readers with the campaign *Capitalism, Time for a Reset*.[149] In addition, in January of 2020, The World Economic Forum in Davos dedicated its 50th edition to rethink stakeholder capitalism, embracing holistic and sustainable economic models to correct the problems created by capitalism itself since the 2008 financial crisis.[150] The Forum did not uttered a clear Manifesto of that nature since the economic crisis in 1973.

The above-mentioned initiatives can be deemed as corporate responsibility, a trend extracted from old manuals for "good" business practices since the 1970s that were reviewed in the context of the recent economic and pandemic crisis. JP Morgan Chase CEO James Dimon, for instance, admitted systemic problems such as

---

[146] As warned by the British theorist R. H. Tawney in 1921.

[147] *Business Roundtable*. 2019. August 19. 'Business Roundtable Redefines the Purpose of a Corporation to Promote 'An Economy That Serves All Americans''. Retrieved from https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans in 03/08/2020.

[148] Light, L. 2017, June 2. 'Why U.S. businesses said "stay in the Paris accord". *CBS News*. Retrieved from https://www.cbsnews.com/news/paris-climate-agreement-us-corporate-support/ in 03/08/2020.

[149] *Financial Times.* 2019, December 30. 'Why capitalism needs to be reset in 2020'. Video description. Retrieved from https://www.ft.com/video/0dae2a4a-8c5c-4718-a540-b1fefae10dc4 in 03/10/2020.

[150] "Capitalism neglected the fact that a company is a social organization, in addition to a profit-oriented entity. This, coupled with the pressures exerted by the financial sector with regard to obtaining short-term results, caused capitalism was increasingly disconnected from the real economy. There are many of us who have seen that this form of capitalism is no longer sustainable" wrote Davos founder Klaus Schwab. See Schwab, K. 2019, December 02. 'Davos Manifesto 2020: The Universal Purpose of a Company in the Fourth Industrial Revolution'. *World Economic Forum*. Retrieved from https://www.weforum.org/agenda/2019/12/davos-manifesto-2020-the-universal-purpose-of-a-company-in-the-fourth-industrial-revolution in 03/10/2020.

the proliferation of social and economic inequality. To correct those problems, he affirms that capitalism should be reinforced to save itself. He understands capitalism as a pure or ideal concept that was never put into practice. Thus, for puritans like him, only by reinforcing "free" competition and the individual initiative one can correct the real system.[151] They promote remedies to the system from within, even if they see themselves as outsiders or exceptions in the economic system. In a network linked to states, bureaucracies, and social movements, their leadership would be able to save the system as they see private initiatives as the purest forms of democracy.

However, the manifestos and the above puritans do not express how the changes in business models would be achieved in the coming time. In addition, those are attempts to foster Humanity in business practices (in the sense of bringing sensibility and alterity with ecosystems and other people), but they barely address the issue of real Legitimacy. That means, the ideal capitalism hardly promotes horizontality and autonomy of normal citizens as active agents that need to participate in the decisions and policies taken in inner circles of corporations. There is not real redefinition to address citizens as active co-decision makers, aside from active customers and consumers. In that sense, the arising question is how to improve the Legitimacy of citizens in companies. Many voices have arisen here. From the so-called radical liberalism (i.e. RadicalXChange Community), progressive capitalism (Stiglitz, 1994), participatory socialism (Piketty, 2014), to economic democracy (Guinan & O'Neill, 2018), all of them affirm that the system has clear failures and needs external changes.

For example, radical liberalism as stated by communities like RadicalXChange rethinks market practices to "uphold fairness, plurality, and meaningful participation in a rapidly changing world".[152] They promote quadrating voting and financing (specialized credits given to citizens to be used as votes), antitrust legislation to combat monopolies, as well as new commissions that mediate data rights from individuals and companies. On the other hand, the traditional economy treated market failures as an exception to the general rule of efficient markets. Yet, in progressive capitalism, Stiglitz theorems postulate market failures as the norm, stating that the government could always improve the distribution of market resources (Stiglitz, 1994). In addition, in participatory socialism, Thomas Piketty proposes horizontal participation in which property becomes temporary whereas assets and fortune circulate permanently. He states that super-millionaires should be subject to a rate on equity of up to 90%, and companies would have to rule their business in terms of co-management (workers

[151] Baker, G. "To Fix Capitalism, We May Need More Capitalism", The Wall Street Journal, retrieved from https://www.wsj.com/articles/to-fix-capitalism-we-may-need-more-capitalism-11556902595 in 09/08/2020

[152] RadicalXChange. Resources and Concepts. Retrieved from https://www.radicalxchange.org/concepts/ in 09/08/2020.

would share power) (2013). It means the overthrow of the "divine right of kings". The French economist seeks to redefine the basic concept of the capitalist system: private property. He aims to transform capital by making it temporary, raising its rotation. It applies to capital the same recipes that it has applied to labor and personal data in the last decades. Finally, from the economic democracy side, Joe Guinan and Martin O'Neill support Community Wealth Building instead of traditional economic development. This consists of local tax incentives and public-private partnerships rather than subsidizing the extraction of profit by footloose corporations with no loyalty to local communities. Community Wealth Building supports democratic collective ownership of the economy through a range of models. These include worker cooperatives, community land trusts, community development financial institutions, so-called "anchor" procurement strategies, municipal and local public enterprise, and public and community banking. Community Wealth Building is an economic system change, but starting at the local level (Guinan & O'Neill, 2018). Although local, those practices are a reality in experiences in our case studies such as in commons and direct economic experiences in Barcelona (Fernández & Miró, 2016), land workers credits, and cooperative projects in Brazil (Singer, 2014).

These experiences can be combined with public administration, private companies, and non-governmental organizations. Yet, Community Wealth Building is different from those actors as they primarily promote horizontality and direct management by broader groups of participants. For example, traditional digital collaborative projects and startups might focus on private revenues, eventually, they can be sold to bigger corporations (a process called *Uberization*). Rather, economic democratic practices escape from that process and maintain their strong bonds with local participants. Yet, they are not the rule and still do not reach the systemic or structural economic level. To reach this level, the accountability principle of "presentation" (continuous direct presence and participation) would be the approach to turn market practices even more horizontal and legitimate.

How to create "presentation" in large market organizations is still a debatable question. Prospective scenarios would need to create an economy based not only on monetarization but also on social outcomes and environmental benefits. It means going beyond standards of responsibility, consultation, and participation. In order to integrate "presentation" forms of governance (real integrations of active and autonomous subjects in the formulation, decision, and implementation of decisions on the large business scale), it is essential to create an alternative economy. According to Tsuruta (2008), this change needs to foster a moral economy and affection economy, an ignored realm that sheds light upon the most vulnerable people and the majority of humans (children and women), as well as underpaid and informal labor. Thin, Verma & Uchida (2017) also call for a system in which trade forms value what our species learned since the dawn of times: to take care of each other. More than rhetoric, this economy means to create

a structure that monitors and obliges (as self-regulation has poorly worked) managers to go beyond the supply of monetary benefits to shareholders.

Even the mentioned Davos Manifesto proposed by Schwab goes in the same logic and emphasizes the need for creating new parameters to measure, produce, and share value, addressing environmental, social, and governance outcomes. The Manifesto affirms that new economic metrics and indicators must be taken into account both at the business level and at the level of public policies to broaden the concept of long-term growth and value. Certainly, there are more initiatives that we cannot address now. Moreover, new ones would emerge to change the ways we understand and measure wealth. And new experiences in economics will be interlinked with public policies and citizens. From ethics to real change, the collision between all those fronts against a form of economics based only on short-term benefits may be what the world needs. Let the fire spark the light; let the multitude enter into the economic structural level. Since accountability is relational and mutable, concrete radical practices still need to be developed. Yet, the path is clear, let the oscillating and porous agency of citizens to be at the center of economy "n+1" times.

Epilogue

This last part complemented the accountability analysis of intelligence and personal data. Here we exposed the importance of metanarratives to orient resistance and alternative forms to construct politics. Metanarratives are the major stories that orient history and humanity. At this level, time and social actors converge to interpret a common path of action (hegemony) and reaction (resistance). This binary division is functional, and must not be interpreted in terms of content and form. That is, the relationship between hegemony and resistance is a complex interaction in surveillance and politics. In terms of actors, there are not only two opposing sides of the divide – one advocating surveillance that the other resists – who are locked in a perpetual cycle of action and reaction. Actors are both complicit in surveillance and can change their roles. However, in terms of function or dynamics for politics, there are two main poles: hegemonic action and resistance agency. Both produce and redefine actors' roles and actions. To use an allegory, that twofold division is similar to the binary system of zeros and ones that constitutes the infinite software and codes in computing.

Since the late twentieth century, metanarratives were deemed as dead and inadequate trends to catch up with the heterogeneity of social practices and epistemologies. The end of metanarratives was uttered after the failure of the epic Icarus model, and by the skepticism of the Sisyphus model. However, taking into account global ethics and the convergence of social, biological, and environmental

crises, local and international, not only metanarratives seem to be necessary today, but they also appear as alternatives to support and connect social changes. Perhaps it is a matter of time until we expect their return.

Considering the theoretical insights from Philosophy, Narratology, and Historiography, we analyzed the legacy of metanarratives since Modernity, their decline in the last century, and the possibilities to reconstruct them in the present time. To do so, as objects, we considered the streams of resistance that hinge on surveillance and politics. Those streams were extracted from the interconnected digital multitude analyzed in Chapter 5. As the destination (teleological) component for political agency or resistance cannot be postulated in absolute terms, we proposed a porous metanarrative that can be triangulated with concrete social practices in order to be "molecular" (micro) and "molar" (macro). This oscillating nature would allow encompassing heterogeneous social practices to orient the quest for new realities, from feasible actions to distant dreams. Future dreams based on Humanity and Legitimacy that need to be rescued/adapted/transformed to reach the core of big transformations in the politics of tomorrow.

In sequence, we have formulated a "political equation" in which we exposed the movement or interaction between authority and agency, revisiting accountability principles. This allows us to give concrete examples of how authority can be redirected to produce new sources of legitimacy. In that operation, we analyzed the flows and the sides of the equation, indicating those sides as ideal typologies that need to be connected in everyday policies. Yet, there is no aim to analyze the content and the form of every form of authority and agency. As indicated in the metanarrative model, we understand that there is no essentialist ontology of authority and agency forms. That is, authority is not per se "bad" nor agency is only "good". Interactions can be transformed into "good" forms of authority and the multitude can enable "bad" and disgusting politics as well.

However, given the metanarrative interpretation of the social reality that overpasses our two case studies, and considering the historical context, the political structure, and the major transformations in surveillance and politics, we equalized authority with top-down lines of capture, and agency with bottom-up lines of escape. From a bigger perspective, in terms of time and relations of power, it is possible to recognize that, despite the array of rhizomes and networks of governance, certain players have more authority and, at the same time, capacity of hegemonic action over other players. If in the past those players were clearly visible in the state, nowadays this image is diluted and blurs with economic and big market players that operate the governance of different issues, including personal data. On the other hand, peripheral groups and players labeled as the multitude do not represent a common front or the automatic answer from powerless people against the powerful ones. This operationalization helps to analyze lines that

challenge and resist to power and hegemony. We still recognize that certain parts of the multitude can work to accelerate or even promote greater levels of hegemony and control. And this is the interesting part of the becoming process of social actors: they do not have essentialist content. Yet, they do have concrete strategies and movements to interact with certain players and against other ones. What the equation represents is the main forms of those strategies and movements, simplifying the "infinite" [153] interactions of people and the different forms of governance. In the array of power relations, what is clear and common to all cultures and societies, is that humans have the capacity to subordinate and rule other people, as well as to react to that domination in many cases. This universal logic can be simplified to an interaction between people from above and people from below (Rüsen, 2005), as represented in the "political equation" (Table 21).

At the same time, this universal logic was directed to the search of Legitimacy, the promotion of human relations (permeated by technology) to encompass equality and horizontality in order to shrink the distance between those from above and below. Meanwhile, Humanity arises as a channel to seek for autonomy and alterity, reshaping the rational and sensible understanding of power. It entails alterity in the difference, the capacity to hear and be heard. It reintroduces the idea of beautiful politics in the tension between those who are authorized to govern and the governed ones.

Authority, as expressed by Hobbes, is the authorization, the license to rule, and is circumscribed to certain conditions that are normative and pragmatic throughout history. When those conditions are violated or appear detached from the original authorization of authority, what needs to be replenished is the content of authority, i.e. by reformative accountability mechanisms. In this change, what needs to be considered is the ideal source of authority, the agency of people. A source that is always there, with vicissitudes and errors, a fundamental entity that is valuable by the potential promises.

Indeed, the multitude is not perfect. Thus, this domain also needs to be transformed and triangulated with greater levels of Humanity and Legitimacy. Agency is modal or relational and needs to point out to a certain telos. Otherwise, it would remain as the heterogeneous mass of people, the loose agglomeration of voices in a cacophony in which there is no room for intelligible music or, what is worse, there is the exclusion of music at all. As molecules oscillate to produce new

[153] "For instance, in the realm of surveillance, the form of how we understand 'benefits' depend on the motivation of whoever is carrying out the surveillance. Increasingly granular knowledge of consumers is a benefit for commercial organizations. Instantaneous access to friends and family via social networking is a benefit for individual Internet users. Capturing communications data is a benefit for law enforcement and the state. The point is that in the entire multitude of arenas defined by the socio-technical system of governance, surveillance is enacted in one form or another, for one purpose or another and – from time to time – it is resisted in one way or another." (Raab, Jones, & Székely, 2015, p. 34).

substances, as the air oscillates to produce sounds, not all the substances are beneficial, not all the sounds are beautiful. Yet, the mode to create substances and to generate sounds can be continuously adapted to refine the very art of producing new materials and melodies. In those efforts, the means and instruments are as important as the ends. To create meaning, the rational tools are as important as the aesthetic dimension to transform everyday politics.

CONCLUSION

"Every child is an artist. The problem is how to remain an artist once one grows up". Pablo Picasso.

In psychological theory, it is said that therapy seeks to facilitate the abandonment of the mental script that people develop in childhood under the influence of parental and authoritarian figures, which is necessary to survive and that people may still be following unconsciously (Erskine, 2018). For example, in Transactional Analysis (TA), those who leave previous scripts stop playing the psychological games that reinforce them. Then, they can use their abilities to think, feel, and act freely, achieving an integrated and healthy life. Not everything constitutes a "good" life. Yet, despite many constraints, a good life, like arts, might be enhanced by everyone.

Naturally, there is a difference between psychological and social dimensions. Yet, in a similar logic, the objective of this study was to examine the development of accountability mechanisms in surveillance in order to: a) preserve and increase the autonomy of individuals subjected to surveillance, b) replenish the asymmetry of power between those who watch and those who are watched.

The point "a" is understood as a basic precondition to enhance any idea of active citizens and "healthy" sociopolitical relationships. It is the capacity to act as an individual and sovereign person in surveillance contexts that can erode not only privacy but also individuality. The point "b" relates to reprogram the relationship between authority and legitimacy in order to leave the "script" inherited by authoritarian legacies and to replenish the increasing political distance between those who watch and are watched. Thus, accountability plays an essential function here as, basically, it can redefine the tension between authority and legitimacy in any sociopolitical order.

In that sense, we addressed two domains or realms to achieve the objectives: intelligence and personal data. We also considered two cases of study: Spain and Brazil since the political transition initiated after authoritarian regimes in the 1970s. Those realms are explained because intelligence refers to exceptional politics whereas personal data relates to normal politics. Yet, exceptionality, the capacity to dictate measures to refund the sociopolitical order, is not disconnected from normality or governmentality, the capacity to prorogue the sociopolitical order. Both capacities intertwine and are not disconnected to execute sovereignty and to calibrate asymmetries of power. For this reason, added to the impossibility to tame completely disgusting politics (see Chapter 1), it was said that accountability has a limited potential or range to restrain power from authority.

Yet, instead of assuming this as a fatalist defeat, accountability modest nature is perhaps its major virtue as it can redefine and refrain power. Thus, we

started with the operationalization of accountability to oversee/restrain intelligence authorities, specifically, strategic intelligence agencies for the security of the state and society.

In the realm of intelligence

Since the 1970s, it was mentioned that due to the struggle between antagonist memories, cosmopolitan memories, and agonistic grounded memories, added to the problem of forgetfulness, the legacy of the authoritarian period is still alive. Moreover, in recent years, the ashes of the repression from the regimes are still warm. However, during the late twentieth century, one must be cautious in associating deviation of power and disgusting politics to intelligence institutions. These institutions were not created as the rational machines of totalitarian states, nor were "improvised" and provisional solutions to the problem of subversion, political dissidence, or terrorism. The institutionalization of information/intelligence agencies represented the construction of coherent answers that Spain and Brazil used to the deployment of "exceptional" measures (exceptional is not necessarily illegal). This potential ability convoked by contemporary bureaucracies can be understood as the epitome of sovereign power who demands specific information for the integrity and preservation of the socio-political order. However, as we have exposed, preserving intertwines and collides with re-foundation. Hence, intelligence tasks could contradict the very sociopolitical order, especially when the foundations of the order change –as in the case of political transitions- or collide disproportionally and unnecessarily against individuals to preserve the order at any cost. Thus, accountability mechanisms were constructed in the last decades to calibrate those services. The first of them was the internal control.

Internal control

In the internal control, the administrative and institutional designs to manage and construct intelligence can be considered as primary forms of accountability. That is, they work as self-restraining mechanisms that governments and administrations deployed over intelligence since the 1970s in each country. In this perspective, we mentioned the institutional evolution of intelligence since the times of political repression to contemporary informational networks. It was also mentioned the creation of specific roles (such as the National Directives of Intelligence in Spain and the National Policy of Intelligence in Brazil) and the administrative law to coordinate the CNI and the SISBIN, as well as auditing channels of supervision and ethical protocols.

Accountability principles promoted: responsibility.

Recommendations: a crucial question here is to avoid the cooptation of the services in the hands of governments, in order to separate this strategic realm

from purely conjectural and partisan issues. At the same time, it is of importance to avoid the transformation of those services into total autonomous institutions, resembling parallel governments outside the control from the Executive. To avoid this, the audits of intelligence should be conducted by independent bodies. Moreover, the figure of ombudsmen must be developed to receive complaints from citizens after wrongdoing and closed operations. This figure also needs to be independent of the Directors of intelligence and establish links with justice Courts. That is, the roles between internal controllers must be reinforced and inserted in a broader community to oversee intelligence, including bodies of other accountability mechanisms and power branches.

Legislative control

In the legislative control of intelligence, the Commissions demanded accountability enacting legislation and constitutional roles, controlling the management of budgets, and approving specific expenditures every fiscal year. Moreover, they established public inquiries and initiatives to call intelligence and the government in secret meetings according to the norms of the Houses. Since legislators usually ignore internal procedures of intelligence, this kind of control was reactive (instead of proactive) and depended on the predisposition of the Executive. See the complete history and analysis of the Commissions in both countries in Chapter 3.

Accountability principles promoted: responsibility and answerability.

Recommendations: In terms of financial oversight, it should be remembered that the budget cycle of public agencies involves at least four steps: 1) elaboration and presentation; 2) legislative approval; 3) execution; 4) evaluation and control (Sanches, 1993 in Mills). Legislators must also consider the latter points to assess intelligence budgets and operations. To do so, Wills (2009) argues that regulations should prohibit services from conducting financial activities not included in the budget. In our vision, governments should make public as much information as they can about the intelligence services without producing harm to public security and national security. Moreover, the Commissions must increase their power to audit all aspects of intelligence, including special accounts related to confidential and closed operations, the links with private companies, and even the cooperation with foreign partners.

Judicial control

In the judicial control of intelligence, the Spanish CNI is accountable to the judicial power through Act 11/2002. According to this, the strategic and national security activities of the CNI that interfere with fundamental rights need to be reported to a Magistrate Judge of the Supreme Court to obtain prior authorization.

In Brazil, the ABIN has no judicial authorization to interfere with fundamental rights, therefore, there is not permanent judicial control.

Accountability principles promoted: responsibility and enforcement

Recommendations: To avoid the problem of over-classification, it is essential to think in advance the restricted audiences that can use classified information for legitimate purposes, such as Parliaments and Courts. We also recommend extending the rules for declassification in Spain (circumscribed to the Council of Ministers) and the implementation of those rules in Brazil. New historical norms to access archives and classified matters also should be created. In Spain, more Magistrates –not only one- should oversee the activities and the measures that are requested by intelligence. In addition, when the judges authorize interventions, they should supervise the deletion of information (especially of data not related to the operations) and verify whether the authorization has been respected and followed (a posteriori control). In Brazil, judicial control should be enabled following the principle of proportionality and indicating the rights that can be interfered with. Current judicial controls focus on target surveillance. Yet, legislation should be developed in both countries to tackle issues related to electronic mass surveillance.

International oversight (Third dimension)

In the accountability of third dimension, intelligence services eventually can justify and clarify the participation/assistance to international players that produced violations against the International Law or against fundamental rights. The Spanish CNI can be indirectly accountable to the Convention Against Torture (CAT), to European regulations and forums (as the Venice Commission and The European Parliament's Committee on Civil Liberties). Intelligence services could be demanded, via domestic and classical forms of accountability, to fulfill international treaties and regulations. In Brazil, the ABIN indirectly follow the CAT and international treaties from the Organization of American States (OAS) and Mercosur despite the lack of official intelligence forums in this region.

Accountability principles promoted: answerability

Recommendations: Innovative mechanisms of accountability such as the creation of new inquiry bodies to the aid of traditional accountability mechanisms should be developed. In that sense, establishing international ad hoc or permanent oversight bodies could provide countries with greater legitimacy and authority to hold states and their services to account. In the absence of such developments, serious doubts remain as to whether national assemblies are appropriate institutions to undertake rigorous investigative work at the international level. On the other hand, intelligence and governments should release reports to the public in two directions. One related to disclose past events. These reports might be

released under the criteria of pen-censorship to avoid conflicts against personal data protection, privacy safeguards, and fundamental rights. The second one relates to reports released by the control bodies from the three powers of the state (see Chapter 3). Both directions should converge to enact a broad *community of intelligence and accountability*, as a deeper step to legitimize the relationship between the state and citizens. Foreign competitors would not benefit from those reports as they can preserve key information and show general plans that are normally undertaken by other states.

Role of the media and civil society

Here, intelligence services were accountable through direct means, such as establishing official communications with society. Moreover, the media enhanced awareness and legitimacy and, in some cases, acted as an investigative and independent watchdog. The indirect means addressed were the role of whistleblowers, leaks and revelations, scholars and journals, and even the role of "pop culture". These forms can spark transparency and other traditional mechanisms of accountability, especially after the revelation of scandals and wrongdoing. Yet, the limitations of these dimensions were attested when the media became an echo chamber (describing general issues rather than assessing substantially the activities of intelligence) or depended on official sources to release a story.

Accountability principles promoted: answerability and transparency

Recommendations: Creation of legal rules to ensure the role of whistleblowers that denounce wrongdoing in the overall administration. In the case of intelligence, the services can increase its legitimacy by considering the role of the media as an enhancer of publicity and information. Finally, it would be valuable if intelligence services open their institutions for deeper reforms. By choosing reframed transparency, or semi-opaqueness, intelligence can show they follow the legal framework imposed by elected policy-makers but also by considering the interest of the society. The agencies might discuss with many citizen commissions the general directives and goals of intelligence every year. And if this field is especially secret in operations and strategies, it can be porous to citizen oversight in its formulation and evaluation. In that sense, the real inclusion of a wide spectrum of different groups, opinions, and perspectives (from practitioners, experts, academics, to non-experts) through the establishment of closed commissions that oversee intelligence and national security may result in a real improvement of legitimacy.

Intersections

In the intersection between surveillance and intelligence, the "panoptic" and the "rhizomatic surveillant assemblage" are more than surveillance metaphors to

analyze intelligence. They represent the flows of information and schemes of power that circulate across different networks. Those flows feed the intelligence assemblage every minute. Hence, this also brings up the challenges to continuously oversee this realm in terms of accountability. Intelligence services such as the CNI and the ABIN are not Big Brother machines that surveille everything and control everybody. Yet, these are central nodes in the rhizomatic constellation of strategic organizations that regulate key flows of information in each country.

The key for intelligence now is not legality, but legitimacy. Therefore, when pathological trends of surveillance are potentially conducted by intelligence, these cannot be effectively restrained by the above accountability mechanisms. Internal and external controls, international actors, and the role of the media and civil society oxygenate but do not tackle the structural layer in which intelligence services act. In other words, the difference of power between watchers of the state and the target groups from the general population, and the relationship between authority and legitimacy that hinges around them, presents a considerable gap hard to be fulfilled. Moreover, one problem is how to calibrate an activity supposed to monitor potential individuals against the establishment (or those who want to alter it even by legitimate means) and radical tactics that could complement and reinforce the accountability of intelligence services. A re-calibration of this balance can oxygenate the limits of accountability in this realm and in general politics. In that logic, to develop societal accountability mechanisms is essential. Currently, intelligence remains a closed realm in the surveillant assemblage that constitutes itself as a cornerstone that sustains the sociopolitical order. Hence, new forms of resistance and active citizenship that challenge the sociopolitical order, and their relationship with intelligence, appear as unexplored issues.

In the realm of personal data:

Since the advent of the Internet, even mundane or normal information such as personal data matter because, for the individuals, it represents the "simulation-redefinition" of their identity and reality, and so of their conditions to live in society. When individuals use or produce data, they can act as passive or active subjects. In addition, every process related to dataveillance starts from a basic step: the ability to collect data, and the capacity to process and create add valued data.

State regulations to protect personal data

Both in Spain and Brazil, personal data protection rules apply to any organization ruled by public or private law, processing data from natural persons, regardless of the means, the country of operation, and the storage of data. Yet, this data must be collected in the territory of those countries. Organizations are accountable to Data Protection Authorities (DPAs) (at European, state, and regional levels in Spain, and at state level in Brazil) about legality, purpose,

confidentiality, integrity, and transparency to process data and by defining specific roles (data subjects, controllers, processors (in both countries) and commissioners (in Spain)). The exception for the regulation is data treatment for particular/private purposes, in cases of statistic research, anonymous data, national defense, state security, investigation and prosecution of criminal and administrative offenses, and the potential use of electronic mass surveillance. In light of that, the DPAs can demand answerability and enforcement principles from data organizations. Answerability refers to recommendations and corrections by soft means, that is, through preventive reforms and corrective measures to abide by specific standards (legality, purpose, confidentiality, integrity) and procedures (risk analysis, information security, and privacy by design techniques). Data organizations will need to follow those measures, otherwise, DPAs can implement accountability by enforcement: hard corrective measures exemplified by administrative and financial fines.

Limits: Despite the devolution of power to implement "good" practices from DPAs to each organization; firstly, the regulations require comprehensive changes to business practices for companies that had not implemented a comparable level of privacy, especially in Brazil. Secondly, one must be skeptical of regulatory mechanisms and "good" practices because they can become fuzzy and elastic enough to be applied to any informational system, like sustainability in the environmental industry. Thirdly, despite the scheme of fines and enforcement, the efficiency to implement accountability may differ extensively in every company. Hence, in overall terms, the data environment can still be "polluted". Finally, responsibility in this domain is diffused as technological developments modify the collection, process, use, and interpretation of data, turning the control of organizations even harder when compared to traditional regulatory arenas such as labor inspection and environmental policies.

Market strategies

In both countries, small and big companies that handle personal data adopted strategies to show accountability. They can report to DPAs, as mentioned above. In this case, the companies have the role to mediate legitimacy promoting rights from users (access, rectification, cancelation, opposition, portability, deletion). Moreover, digital data companies can report to enforcement authorities (administrative and from justice) as in the case of the Facebook and Google Transparency Reports analyzed in Spain and Brazil. Furthermore, companies can report through four layers of accountability: 1. in the public frontend layer, to monitor and delete information by default, 2. in the private frontend layer, to monitor and delete information by default or under the pressure of authorities, 3. in the backend layer, to deliver metadata under administrative request ("less" sensitive information of users), 4. in the backend layer, to deliver core data under judicial warrants (content and sensitive information of users). Additional

accountability forms in the market include good practices such as system security maintenance, enabling customers' services, auditing algorithms, and adopting Privacy by design principles.

Limits: In the transparency reports, companies still can bargain power to preserve their internal policies, such as intellectual property and industrial secrecy. For instance, it is difficult to conclude if Facebook and Google are really accountable by the information they release (when enforcement agencies need specific data as proof for trials and judicial actions). That is, the corporations can cooperate with public authorities by default, labeling this collaboration as "transparency". We also mentioned that accountable algorithms still depend on an investigative journalistic culture to assess data sets, correct biases, and clarify the data correlations. Given the proliferation of algorithms and data business, in public and market domains, more proactive and transparent measures need to be taken in the next decades. Furthermore, to verify transparency, the metaphor of "slides of visibility" explained in Chapter 5 is useful to criticize transparency schemes in the governance of personal data. In the current scheme, users are more transparent to big data processors such as Google, but the reversal is not true. Companies became friendly and trustworthy platforms, but little transparency (aside from user setting tools and overall guidelines shared by default) exists from data processors to users. Finally, due to the pressure of enforcement agencies to share data, the pressure of other competitors, and the pressure from shareholders to obtain revenues, giant data processors manage their multiple mechanisms of accountability in favor of also powerful players (public authorities and market shareholders). This leaves behind more commitment to favor users and citizens to shape the business sector.

Civic agency

The impact of civic agency (the connected-multitude) to enhance accountability is still debatable. Many critiques could arise because of the array of responses and lack of a common orientation to resistance. Yet, the civic multitude can oxygenate transparency, responsibility, answerability, and even spark enforcement principles in other domains of governance. Besides, the multitude must be understood in plural terms and especially by the mutable modulation of relations of power. This is the most flexible domain as the multitude strategies are mutable and the collective actions hinge on the adaptation of tactics, people, and goals.

In this domain, we identified four streams of resistance: 1) Ironic stream: based on discourse and aesthetics, such as humor, communication, and arts. 2) Deliberative stream: based on cooperation, such as Digital correct activism, open codes, commons, and public consultation. 3) Agonistic stream: based on confrontation, such as Digital mass Hacktivism, DDoS attacks, whistleblowing, and

boycott. 4) Despair stream: based on high conflict, such as protests, riots, and unrest. We also mentioned that the ironic and deliberative streams tend to focus on the agency level (actors), whereas the agonistic and despair streams tend to focus on the structural level (macro-political context). The structural level means actors and strategies that go beyond surveillance and address changes in the whole sociopolitical order. Also, the streams have interdependence and their synchronization appears in key moments of history, such as in the Spanish and Brazilian revolts in 2011 and 2013. Moreover, the streams can be coopted or hijacked by counter-resistance measures.

It is important to remind that the tactics and streams of resistance are not necessarily illegitimate, even if they are illegal. The sources of legitimacy stem from the multitude. Yet, even when resistance is distorted by illegitimate means, this does not justify illegitimate counter-resistance and unaccountable answers for the sake of security or to normalize the social order. From humor narratives against the establishment, to massive riots and unrest tactics, the assessment of the streams should be carefully conducted during/after concrete actions and outcomes. This demands more attention to scrutinize preemptive and automated surveillance tools.

Intersections

In the intersection between surveillance and personal data, good practices (such as market strategies centered in users, privacy by design, risk analysis, and security of information) converge in a paradigm that hinges on the care of ourselves, in caring our reputation and image, rather than in promoting hard disciplinary means of control.

In that sense, the first driving force in surveillance nowadays goes beyond the theoretical ideas of social control and relates to the differentiation of social systems and to the continuous demands to generate new sets of data, especially through giant data processors that took the first position in the global market.

The second driving force in surveillance is the response from big market players to give orientation to the production and monitoring of data. In the last decades, they focused on the direct collection and monitoring of data from the sources of information: people. Besides being a source of production and labor, a population has become, at the same time, a reserve of information that can be better 'exploited' for the performance of the dataveillance assemblage. This exploitation does not necessarily take the commodity form. Populations are also potential sources to feed the pipelines of information beyond the ideas of governmentality. Data subjects are valuable because of their constitution: they are subjects *of* data.

Finally, the governance of personal data also entails social differentiation, social systems, and social position between players. This domain alters biopolitics redefining the prefix "bio", from pure organic bodies, to power oscillations that reshape individuality and the social reality. Biopolitics extrapolates the differentiation of social systems that assemble cyborg-bodies and surpasses previous ideas of simulation and reality. Yet, in that oscillation and flexibility, power and normality are not equally distributed and clashes emerge, reworking the notions of resistance.

Postscript on the societies of surveillance:

The last part complemented the analysis of accountability in the realms of intelligence and personal data. This part exposed the importance of metanarratives to orient resistance and alternative forms to construct politics. Metanarratives are the major stories that orient history and humanity. At this level, time and social actors converge to interpret a common path of action and reaction (resistance).

We analyzed the legacy of metanarratives since Modernity, their collapse in the last century, and the attempts of reconstruction in the present time. Taking into account global ethics and the convergence of social and environmental crises, from local to international governance, not only metanarratives seem to be necessary today, but they also appear as alternatives to support and connect social changes in the long future.

In order to reconstruct a metanarrative, we considered the streams of resistance that hinge on surveillance and politics. As the destination (teleology) of resistance cannot be postulated in absolute and uniform terms, we propose a porous metanarrative that can be triangulated with concrete social practices. This would allow encompassing heterogeneous practices to orient the quest for new realities, from feasible actions to those that belong to the domain of dreams. Dreams based on Legitimacy and Humanity that need to be rescued/adapted/transformed in order to reach the core of big transformations in tomorrow politics.

Legitimacy is the promotion of social relations (permeated by technology) that comprise intrinsic equality and horizontal power relations, shrinking the distance between those from "above" and "below", powerful and powerless. Meanwhile, Humanity relates to individual autonomy and alterity with other social groups and nature. It also relates to the rational and aesthetic dimensions to calibrate power, highlighting the ability to hear and be heard. It entails alterity in the difference. It reintroduces the idea of beautiful politics to manage the tension between those who are authorized to govern and the governed ones.

Considering the reconstruction of a metanarrative, in sequence, we have formulated a "political equation" in which we exposed the movement or

interaction between authority and agency, revisiting accountability principles. In that sense, we formulated further or radical accountability principles (representation, consultation, participation, and presentation) that can be triangulated with concrete practices and beliefs in order to promote more levels of Legitimacy and Humanity. The institutionalization and achievement of this triangulation still needs to be explored and is open to further experiences. Yet, we offered concrete examples showing forms in which authority can be redirected to produce new sources of legitimacy both in intelligence agencies and personal data. For example, intelligence might be exceptional in terms of methods and implementation, but it can be deeply scrutinized by new citizen commissions in the formulation and evaluation.

In a broader perspective, in terms of time and relations of power, it is possible to recognize that, despite the array of rhizomes and networks of governance, certain players have more authority and, at the same time, capacity of hegemonic action over other players. If in the past those players were clearly visible in the state, nowadays this image is diluted and blurs with economic and big market players that operate the governance of different issues, including personal data. On the other hand, peripheral groups and players labeled as the multitude do not represent a common front or the automatic answer from powerless people against the powerful ones. This operationalization helps to find lines that challenge and resist to power and hegemony. We still recognize that certain parts of the multitude can also work to accelerate or even promote greater levels of capture, of hegemony, and social control. And this is the interesting part of the becoming process of social actors: they do not have ultimate lines or immanent essence. Neither authority is “bad” per se, nor is the multitude “good”. Notwithstanding, the civic agency is closely related to the ideal source of legitimacy. The fragmented and heterogeneous multitude, with vicissitudes and mistakes, is virtually the fundamental value that sustains the promises of political legitimacy. Eventually, it can sustain macro projects to recalibrate asymmetries of power and enhance new forms of individual autonomy.

As seen in this study, surveillance is able to mediate power through the collection, process, analysis, and use of information from individuals. The mediation of power is not unidirectional and is also altered by flexible strategies of actors. That is, surveillance also entails processes of codification and decodification, as expressed by Stuart Hall (2001). Challenging all components of the mass communications model, Hall argued that meaning is not simply fixed or determined by the sender, the message is never transparent; and the audience is not a passive recipient of meaning. He suggests that distortion is built into the system, rather than being a "failure" of the producer or viewer. Thus, there is a "lack of fit” between the moment of the production of the message (encoding) and the moment of its reception (decoding).

However, current surveillance also challenges the separation between encoding and decoding. As discussed in the "prosumer" idea of users' commodification, individuals become simultaneously producers and consumers of content. There are more flexible schemes and relations to encode and decode the reception of messages. Also, there are more tools to abstract individuals from their individualities, recombining fragments of their data to recreate meaning and representation. In that sense, the representation of individuals' information through surveillance is similar to the House of Mirrors metaphor: the process of collecting, sorting, rendering, and even distorting subjects through data.

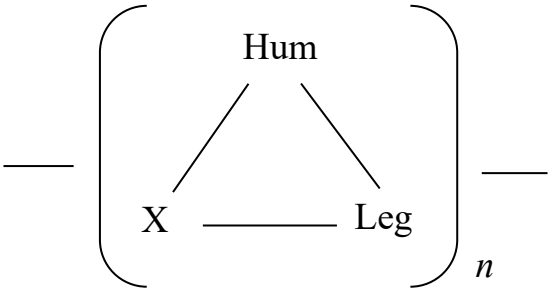
Thus, another importance of the metanarrative consists in recognizing that the ground for the civic agency is not lost because of the recombination and abstraction of individuals. We propose a metanarrative in which a negative ontology (lack of fixed identity) does not constitute a final obstacle to resistance and contestation. The interconnected multitude can use encoding/decoding strategies to reconstitute the access to information and replenish their social position as active agents. This is the case, for example, of sociotechnical interventions through streams of resistance as analyzed in Spain and Brazil. The lack of total synchronization between "dividuals" or data-doubles, as expressed by Deleuze, and individuals, does not close the door to resistance opportunities.

However, resistance actions and the recalibration of power asymmetries are hard to be accomplished insofar as plenty of reasons can override the search for legitimacy in surveillance and politics. In the worst-case scenario, parliamentary controls can be weak, judicial controllers might lack independence, the media role can be coopted, data protection regulations can be insufficient, market strategies can be fuzzy, and civic agency strategies can fail. That is, disgusting politics can be promoted by hundreds of reasons and motives. As explained at the beginning of this work, disgusting politics (such as intrusive surveillance, lack of legitimacy, and technical and utilitarian authority with no controls) are self-referential and cannot be fully controlled or totally counteracted by beautiful politics (such as efficient accountability, proportional legislation, legitimate resistance, and even ethics). However, beautiful politics can redefine the disgusting ones and produce more politics based on Legitimacy and Humanity, as explained in the last part. This resembles the importance to improve the different accountability mechanisms exposed in this study. But it also calls for further actions and radical attempts to redirect power asymmetries in surveillance and beyond. Even in conservative and progressive perspectives, things must change either to preserve things the way they are or to achieve new realities. In that sense, changes can be promoted by continuous redefinitions of authority via accountability actions, from reformative to radical principles that enlarge the participation and presence of citizens in politics and economy.

To recalibrate power, both Legitimacy (equality and horizontality) and Humanity (autonomy-alterity and rational-aesthetical sensibility) remind us that exceptional politics are not disconnected from normal politics. Even the most exceptional changes in History hinge on new forms of normalization, continuity, and routinization. In that sense, tiny or normal actions also matter. The micropolitics of every day is also attached to exceptional changes to wake up new realities. Thus, even the common and individual actions of the reader matter. From collective actions to personal habits, the reader is also an agent to construct and restrain power.

In the differentiation of social systems, including surveillance, the rhizomes spread liked nodes in a network to propagate new fields, new "stems" and "buds". The rhizomatic assemblage is the vertical and horizontal expansion of informational threads and networks. In botanic, if a rhizome is separated each piece may be able to give rise to a new plant. The ability to easily grow rhizomes depends on plant hormones and biotic conditions. That is, the functions of the rhizomes can be reprogrammed. In a similar sense, the rhizomatic nodes of surveillance can be reprogrammed by the capillarity of accountability practices; from the legal reform of giant organizations to the oversight of tiny codes of algorithms and automated machines; from permanent institutional designs to contingent actions of the multitude.

This re-programming depends on the triangulation between Humanity (Hum), Legitimacy (Leg), and concrete practices ("X") *n* times. It is up to us to insert the content and amplitude of those practices to produce "political polymers" that enhance molecular and molar changes, redefining the meaning and reconnecting fields in the accelerated sociotechnical differentiation of our era.



References

Aba-Catoira, A. (2002). El secreto de Estado y los servicios de inteligencia. *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol, (38)*, 133-168.

Agamben, G. (1998). *Homo sacer: Sovereign power and bare life.* Stanford, CA: Stanford University Press.

Agamben, G. (2016). *The use of bodies.* Standford, CA: Stanford University Press.

Alcazan, A., Axebra, Q., Levi, S., SuNotissima, T., & Toret, J. (2012). *Tecnopolítica internet y r-evoluciones. Sobre la centralidad de las redes digitales en el M, 15.* Madrid: Icaria Editorial.

Almenara, V. (2012). *Los servicios de inteligencia en España: de Carrero Blanco a Manglano.* Madrid: Arcopress.

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New media & society, 20(3)*, 973-989.

Andrejevic, M. B. (2011). Surveillance and alienation in the online economy. *Surveillance & Society, 8(3)*, 278-287.

Antunes, P. C. (2002). *SNI & ABIN: Entre a teoria e a prática. Uma leitura da atuação dos Serviços Secretos.* Rio de Janeiro: FGV Editora.

Antunes, P. C. (2004). O estabelecimento do controle público da Atividade de inteligência no Brasil: um grande desafio. *Latin American Studies Association, XXV International Congress, Brazil´s Foreig policy, October 07-09.* Las Vegas, Nevada, USA.

Aradau, C., & Blanke, T. (2010). Governing circulation: A critique of the biopolitics of security. *Security and Global Governmentality*, 56-70.

Aradau, C., & Van Munster, R. (2007). Governing terrorism through risk: Taking precautions,(un) knowing the future. *European journal of international relations, 13(1)*, 89-115.

Arendt, H. ((1951) 1973). *The origins of totalitarianism.* Boston: Houghton Mifflin Harcourt.

Arroyo, G. (1997). El valor probatorio de los Papeles del Cesid. *Cambio 16, (1323)*, 21.

Arturi, C. S., & Rodriguez, J. C. (2011). Controles democráticos e serviços de inteligência e de segurança interna em Portugal e no Brasil. In Cepik, M. *Inteligência Governamental: contextos nacionais e desafios contemporâneos* (pp. 3-46). Niterói: Impetus.

AsimAkopoulos, J. (2016). A radical proposal for direct democracy in large societies. *Brazilian Journal of Political Economy, 36(2)*, 430-447.

Avila, A. P., & Woloszyn, A. L. (2017). Legal protection of privacy and confidentiality in the digital era: doctrine, legislation and jurisprudence. *Revista de Investigações Constitucionais, 4(3),* 167-200.

Awan, A. (2014). Brazil's innovative anti-poverty & inequality model. *American Journal Of Trade And Policy, 1(3)*, ss.

Badiou, A. (2014). *Théorie du sujet.* Paris: Le Seuil.

Bakir, V., & McStay, A. (2015). Assessing interdisciplinary academic and multi-stakeholder positions on transparency in the post-Snowden leak era. *Ethical Space, 12(3/4),* 25-38.

Bal, M., & Marx-MacDonald, S. (2002). *Travelling concepts in the humanities: A rough guide.* Toronto: University of Toronto Press.

Ball, K. (2005). Organization, surveillance and the body: Towards a politics of resistance. *Organization, 12(1)*, 89-108.

Balzacq, T. (2011). *Securitization theory: How security problems emerge and dissolve.* London: Routledge.

Barber, B. ((1984) 2003). *Strong democracy: Participatory politics for a new age.* Los Angeles, CA: University of California Press.

Barel, E., Van IJzendoorn, M. H., Sagi-Schwartz, A., & Bakermans-Kranenburg, M. J. (2010). Surviving the Holocaust: a meta-analysis of the long-term sequelae of a genocide. *Psychological bulletin, 136(5)*, 677-692.

Barrilao, J. F. (2019). Servicios de inteligencia, secreto y garantía judicial de los derechos. *Teoría y realidad constitucional, (44)*, 309-340.

Bartczak, K. (2015). Richard Rorty and the ironic plenitude of literature. *Contemporary pragmatism, 12(1)*, 59-78.

Baudrillard, J. ((1981) 1994). *Simulacra and simulation.* Ann Arbor: University of Michigan press.

Bauman, Z. (1992). *Intimations of postmodernity.* London: Routledge.

Bauman, Z. (1999). *In search of politics.* Stanford, CA: Stanford University Press.

Bauman, Z. (2000). *Liquid modernity.* Hoboken, NJ: John Wiley & Sons.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation.* New Jersey: John Wiley & Sons.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International political sociology, 8(2)*, 121-144.

Bayer, M. D. (2010). *The blue planet: Informal international police networks and national intelligence.* Washington DC: Government Printing Office.

Bean, H. (2013). Rhetorical and critical/cultural intelligence studies. *Intelligence and National Security, 28(4),* 495-519.

Bean, H. (2018). Intelligence theory from the margins: questions ignored and debates not had. *Intelligence and National Security, 33(4)*, 527-540.

Beck, U. (1992). *Risk society: Towards a new modernity.* New York: Sage.

Beer, D., & Burrows, R. (2010). Consumption, prosumption and participatory web cultures: An introduction. *Journal of Consumer Culture 10(1)*, 3-12.

Belli, L., & Foditsch, N. (2016). Network neutrality: An empirical approach to legal interoperability. *Net Neutrality Compendium*, 281-298.

Benet, J. (1979). *Cataluña bajo el régimen franquista.* Barcelona: Blume.

Bennett, J. (2003). The aesthetics of sense-memory: Theorising trauma through the visual arts. *In Regimes of memory*, 40-52.

Benton, T. (1984). *The Rise and Fall of Structural Marxism: Louis Althusser and His Influence.* New York: Macmillan International Higher Education.

Berlin, I. (2017). Two concepts of liberty. *Liberty Reader*, 33-57.

Best, V., & Robson, K. (2005). Memory and innovation in post-Holocaust France. *French studies, 59(1)*, 1-8.

Beverley, J. (2011). Repensando la lucha armada en América Latina. *Sociohistórica, (28)*, 163-177.

Bezerra, A. C. (2017). Surveillance and algorithmic culture in the new global regime of information mediation. *Perspectivas em Ciência da Informação, 22(4),* 68-81.

Bigo, D. (2008). Globalized (in) security: the field and the ban-opticon. *Terror, insecurity and liberty*, 20-58.

Bigo, D. (2015). Vigilancia electrónica a gran escala y listas de alerta: ¿Productos de una política paranoica? *REMHU: Revista Interdisciplinar da Mobilidade Humana, 23(45)*, 11-42.

Bigo, D., Carrera, S., Hernanz, N., & Scherrer, A. (2015). *National security and secret evidence in legislation and before the courts: exploring the challenges.* Brussels: Centre for European Policy Studies.

Bjola, C., & Pamment, J. (2018). *Countering online propaganda and extremism: The dark side of digital diplomacy.* London: Routledge.

Blaug, R. (2002). Engineering Democracy. *Political Studies*, 50(1), 102–116.

Bobbio, N. (1987). The future of democracy: A defence of the rules of the game. Minneapolis: University of Minnesota Press.

Bobbio, N. (1989). Gramsci and the concept of civil society . In Keane, J. *Civil society and the state. New European Perspectives.* London: Verso books.

Bogard, W. (1996). *The simulation of surveillance: Hyper-control in telematic societies.* Cambridge: Press Syndicate of the University of Cambridge.

Borelli, S. (2003). Terrorism and human rights: Treatment of terrorist suspects and limits on international co-operation. *Leiden Journal of International Law, 16(4)*, 803-820.

Borges, N. (2003). A Doutrina de Segurança Nacional e os governos militares. O tempo da ditadura: regime militar e movimentos sociais em fins do século XX. In J. Ferreira, & L. D. Delgado, *O tempo da ditadura: regime militar e movimentos sociais em fins do século XX* (pp. 13-42). Rio de Janeiro: Civilização Brasileira.

Born, H., & Leigh, I. D. (2005). *Making intelligence accountable: legal standards and best practice for oversight of intelligence agencies.* Oslo: Publishing House of the Parliament of Norway.

Born, H., & Wills, A. (2011). International responses to the accountability gap: European inquiries into illegal transfers and secret detentions. In H. Born, I. Leigh, & A. Wills, *International Intelligence Cooperation and Accountability* (pp. 211-240). London: Routledge.

Born, H., Leigh, I., & Wills, A. (2011). *International intelligence cooperation and accountability.* London: Routledge.

Botto, M. (2015). América del Sur y la integración regional: ¿Quo vadis? Los alcances de la cooperación regional en el Mercosur. *Confines de relaciones internacionales y ciencia política, 11(21)*, 9-38.

Bourbeau, P. (2014). Moving Forward together: Logics of the securitization process . *Millennium: Journal of International Studies, 43 (1)*, 187-206.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, 15(5), 662-679.

Boyne, R. (2000). Post-panopticism. *Economy and Society, 29(2)*, 285-307.

Boyte, H. C. (2005). Reframing democracy: Governance, civic agency, and politics. *Public Administration Review, 65(5)*, 536-546.

Bozdag, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and information technology*, 15(3), 209-227.

Bozdag, E., & van den Hoven, J. (2015). Breaking the filter bubble: democracy and design. *Ethics and Information Technology*, 17(4), 249-265.

Braithwaite, J. (2006). Accountability and responsibility through restorative justice. In Dowdle, M. D., *Public accountability: Designs, dilemmas and experiences*, 33-51. Cambridge: Cambridge University Press.

Brandao, P. (2019). Amerino Raposo e a Polícia Federal. *Faces da História, 6(1)*, 246-270.

Brassier, R. (2008). *Nihil unbound: naturalism and anti-phenomenological realism.* London: Palgrave-Macmillan.

Braund, S. H. (1992). Juvenal—misogynist or misogamist? *The Journal of Roman Studies, 82*, 71-86.

Brennan, T. (2010). Net neutrality or minimum quality standards: Network effects vs. market power justifications. *Market Power Justifications (June 8, 2010).*

Bueso, J. C. (1997). Información parlamentaria y secretos oficiales. *Revista de las Cortes Generales*, 7-34.

Burgos, A. (2016). *Political philosophy and political action: Imperatives of resistance.* London: Rowman & Littlefield.

Burles, R. M. (2016). Exception and governmentality in the critique ofsovereignty. *Security Dialogue, 47(3)*, 239-254.

Busuioc, M., & Groenleer, M. (2013). Beyond design: The evolution of Europol and Eurojust. *Perspectives on European Politics and Society, 14(3)*, 285-304.

Butler, J. ((1990) 2011). *Gender trouble: Feminism and the subversion of identity.* Abingdon: Routledge.

Buzan, B. (2003). Regional security complex theory in the post-cold war world. In F. Söderbaum, & T. M. Shaw, *Theories of new regionalism*, 140-159. London: Palgrave Macmillan.

Caldeira, T. P. (2000). *City of walls: crime, segregation, and citizenship in São Paulo.* Los Angeles, CA: University of California Press.

Calise, M., & Lowi, T. J. (2010). *Hyperpolitics: an interactive dictionary of political science concepts.* Chicago: University of Chicago Press.

Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. *Social Identities, 16(5)*, 621-633.

Campbell, D. (2000). Global surveillance: the evidence for Echelon. *Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions*, 149-154.

Caparini, M. (2004). Media and the security sector: Oversight and accountability. *Geneva Centre for the Democratic Control of Armed Forces (DCAF) Publication*, 1-49.

Caparini, M. (2016). *Democratic control of intelligence services: containing rogue elephants.* New York: Routledge.

Caputo, J. D. (2003). Without sovereignty, without being: Unconditionality, the coming God and Derrida's democracy to come. *Journal for Cultural and Religious Theory, 4(3)*, 9-26.

Carpentieri, J. R. (2016). *Inteligência e direito: O caso do Sistema Brasileiro de Inteligência.* Sao Paulo: Doctoral Dissertation, Universidade Presbiteriana Mackenzie.

Carroll, D. (1990). *Paraesthetics: Foucault, Lyotard, Derrida.* New York: Collman.

Casanova, J., Fontana, J., & Villares, R. (2007). *República y guerra civil.* Barcelona: Crítica/Marcial Pons.

Castells, M. (2004). *The network society: A cross-cultural perspective.* Northampton, MA: Edward Elgar Publishers.

Castells, M. (2013). *Redes de indignação e esperança: movimentos sociais na era da internet.* Rio de Janeiro : Zahar.

Castro, C., & D'Araujo, M. C. (2001). *Militares e política na Nova República.* Rio de Janeiro: FGV Editora.

Cavatorta, F., & Pace, M. (2010). Post-Normative turn in European Union (EU)-Middle East and North Africa (MENA) relations: An Introduction. *The. Eur. Foreign Aff. Rev., 15, 581*, 581-ss.

Cavoukian, A. (2009). *Privacy by design. Take the challenge*. Information and privacy commissioner of Ontario, Canada.

Cawthra, G., & Luckham, R. (2003). *Governing insecurity: Democratic control of military and security establishments in transitional democracies.* London: Zed Books.

Cepik, M. (2003). *Espionagem e democracia.* Rio de Janeiro: FGV Editora.

Cepik, M., & Möller, G. (2017). National intelligence systems as networks: power distribution and organizational risk in Brazil, Russia, India, China, and South Africa. *Brazilian Political Science Review, 11(1)*, Epub March 27, 2017.

Claret Miranda, J. (2006). *El atroz desmoche. La destrucción de la Universidad española por el franquismo, 1936-1945.* Barcelona: Crítica.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31(5),*, 498-512.

Clarke, R. (1994). The digital persona and its application to data surveillance. *The information society, 10(2),* 77-92.

Cole, D. (2009). Out of the shadows: Preventive detention, suspected terrorists, and war. *California Law Review, 97(3)*, 693-750.

Coleman, S., & Blumler, J. G. (2009). *The Internet and democratic citizenship: Theory, practice and policy.* Cambridge: Cambridge University Press.

Collier, R. B., & Collier, D. (1991). *Critical junctures and historical legacies.* Princeton: Princeton University Press.

Collier, S. J., & Lakoff, A. (2008). Distributed preparedness: the spatial logic of domestic security in the United States. *Environment and planning D: Society and space, 26(1)*, 7-28.

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). *The business of platforms: Strategy in the age of digital competition, innovation, and power.* New York: HarperCollins.

Da Silveira, S. A. (2013). Aaron Swartz and the battles for freedom of knowledge. *SUR-International Journal on Human Rights, 18, 7*, ss.

Dagnino, E. (2008). Civic driven change and political projects. In Fowler, A, & Biekart, k. *Civic driven change: Citizen's imagination in action*, 27–49. The Hague: Institute of Social Studies.

Dahl, R. A. (1989). *Democracy and its critics.* Hartfort, CO: Yale University Press.

Daidj, N. (2019). Uberization (or uberification) of the economy. *Advanced Methodologies and Technologies in Digital Marketing and Entrepreneurship. IGI Global*, 116-128.

Daly, A. (2017). Beyond 'hipster antitrust': A critical perspective on the European Commission's Google Decision. *European Competition and Regulation Law Review, 1 (3)*, 188-195.

Dandeker, C. (1990). *Surveillance, power and modernity: Bureaucracy and discipline from 1700 to the present day*. New York: Polity.

D'Araújo, M. C., Soares, G. A., & Castro, C. (1994). *Os Anos de Chumbo: a memória militar sobre a repressão.* Rio de Janeiro: Relume-Dumará.

Dardot, P., & Laval, C. (2014). *The new way of the world: On neoliberal society*. London: Verso Trade.

David, P. A. (2007). Path dependence: a foundational concept for historical social science. *Cliometrica,1(2)*, 91-114.

Davis, J. W., & Meckel, M. (2013). Political Power and the Requirements of Accountability in the Age of WikiLeaks. *ZPol Zeitschrift für Politikwissenschaft, 22(4)*, 463-491.

Davis, M. (1998). *Ecology of fear: Los Angeles and the imagination of disaster.* New York: Macmillan.

Davis, S., & Straubhaar, J. (2020). Producing Antipetismo: Media activism and the rise of the radical, nationalist right in contemporary Brazil. *International Communication Gazette, 82(1)*, 82-100.

De Carvalho, J. M. (2019). *Forças Armadas e política no Brasil.* Rio de Janeiro: Zahar Editora.

De Montesquieu, C. ((1748) 1989). *The spirit of the laws.* Cambridge: Cambridge University Press.

De Oliveira, E. R. (1987). *As forças armadas no Brasil (Vol. 7).* Sao Paulo: Espaço e Tempo.

De Souza, F. F. (2011). Operação Condor: Terrorismo de estado no Cone Sul das Américas. *AEDOS, 3(8)*.

Debord, G. ((1967) 2012). *Society of the spectacle.* London: Bread and Circuses Publishing.

Deleuze, G. (1995). Postscript on control societies. *Negotiations: 1972–1990, 1995.*, 177-182.

Deleuze, G., & Guattari, F. (1988). *A thousand plateaus: Capitalism and schizophrenia.* London: Bloomsbury Publishing.

Delgado, L. D., & Ferreira, J. (2003). *O Brasil republicano.* Rio de Janeiro: Civilizacao brasileira.

Delpeuch, T., & Ross, J. E. (2016). *Comparing the democratic governance of police intelligence: New models of participation and expertise in the United States and Europe.* Boston, MA: Edward Elgar Publishing.

Dencick, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society, 2016*, 1-12.

Derrida, J. (1978). *Cogito and the history of madness.* Chigaco: University of Chicago Press.

Derrida, J. (1978). *Writing and difference.* Chicago: University of Chicago Press.

Derrida, J. (2010). *The beast and the sovereign (Vol. 1).* Chicago: University of Chicago Press.

Diakopoulos, N. (2015). Accountability in algorithmic decision-making. *Queue, 13(9)*, 1-24.

Díaz-Fernández, A. M. (2005). *Los servicios de inteligencia espanoles/The intelligence services of Spain: Desde la guerra civil hasta el 11-M, Historia de una transicion/From the civil war through the 11-M, History of a transition.* Madrid: Anaya-Spain.

Díaz-Fernández, A. M. (2006). El servicio de inteligencia español a la luz de la teoría de la organización. *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol n. 48*, 19-39.

Díaz-Fernández, A. M. (2006b). El servicio de inteligencia: un actor político en la transición española. *Studia Historica. Historia Contemporánea, 23*.

Díaz-Fernández, A. M. (2010). The need and role of intelligence services in a democracy: Balancing effectiveness and transparency. *paper commissioned for course NS3155.* Monterey, CA.: Naval Postgraduate School.

Díaz-Fernández, A. M. (2013). *Diccionario LID Inteligencia y seguridad.* Madrid: LID Editorial Empresarial.

Díaz Pita, M. D. (1997). *El bien jurídico protegido en los nuevos delitos de tortura y atentado contra la integridad moral.* Universidad de Sevilla: Actas.

Diken, B., & Carsten, B. L. (2002). Zones of indistinction: Security, terror,and bare life. *Space and culture 5, no. 3*, 290-307.

Diken, B., & Laustsen, C. B. (2005). The culture of exception: Sociology facing the camp. *Psychology Press*.

Dörr, K. N., & Hollnbuchner, K. (2017). Ethical challenges of algorithmic journalism. *Digital journalism, 5(4)*, 404-419.

Dowdle, M. D. (2006). *Public accountability: Designs, dilemmas and experiences.* Cambridge : Cambridge University Press.

Dreifuss, R. A., & Dulci, O. S. (1983). As Forças Armadas e a política. In M. H. Almeida, & B. Sorj, *Sociedade e política no Brasil pós-64.* Sao Paulo: Brasiliense.

Dyson, F. (1979). *Disturbing the universe.* New York: Basic Books Inc.

Eder, F. (2011). The European Union's counter-terrorism policy towards the Maghreb: trapped between democratisation, economic interests and the fear of destabilisation. *European Security, 20(3)*, 431-451.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review, 14(4)*, 532-550.

Emirbayer, M., & Mische, A. (1998). What is agency? *American journal of sociology, 103(4)*, 962-1023.

Encarnación, O. G. (2007). Democracy and dirty wars in Spain. *Human Rights Quarterly*, 950-972.

Erskine, R. G. (2018). *Life scripts: A transactional analysis of unconscious relational patterns*. New York: Routledge.

Esposito, R. (2013). *Terms of the political: Community, immunity, biopolitics.* New York: Fordham University Press.

Esteban Tejedor, E. (2018). *El proceso secesionista catalán en televisión. El referéndum del 1 de octubre de 2017 en TVE y La Sexta.* Valladolid: Trabajo Fin Grado Periodismo. Facultad de Filosofía y Letras. Universidad de Valladolid.

Estévez, E. E. (2000). Estructuras de control de los sistemas, organismos y actividades de inteligencia en los estados democráticos. *Primer Seminario Internacional: La Inteligencia en las Organizaciones del Siglo XXI.* Santiago de Chile: Universidad de Chile.

European Information Society Forum Report, (1999). Connecting to the information society: a European perspective. Stephanidis C., & Emiliani, P. L. (Eds.). *Technology and disability*, 10(1), 21-44.

Falque, J. R. (2005). Los servicios de inteligencia en la historiografía española. *Arbor, 180 (709)*, 25-74.

Farson, A. S., Stafford, D., & Wark, W. K. (1991). *Security and intelligence in a changing world: new perspectives for the 1990s.* Oxfordshire: Psychology Press.

Feigenbaum, J., & Ford, B. (2015). Seeking anonymity in an internet panopticon. *Communications of the ACM, 58(10)*, 58-69.

Fernández, A., & Miró, I. (2016). *La economía social y solidaria en Barcelona.* Barcelona: Montaber.

Fernández-García, N. (2017). Fake news: una oportunidad para la alfabetización mediática. *Nueva sociedad, (269)*, 66-77.

Fernández-Quijada, D., & Arboledas, L. (2013). The clientelistic nature of television policies in democratic Spain. *Mass Communication and Society, 16(2)*, 200-221.

Fico, C. (2001). *Como eles agiam: os subterrâneos da Ditadura Militar: espionagem e polícia política.* Rio de Janeiro: Editora Record.

Fico, C. (2008). *Ditadura e democracia na América Latina: balanço histórico e perspectivas.* Rio de Janeiro: FGV Editora.

Fisher, M. (2014). *Ghosts of my life: Writings on depression, hauntology and lost futures.* London: John Hunt Publishing.

Fishkin, J. S. (1991). *Democracy and deliberation: New directions for democratic reform.* New Haven, CT: Yale University Press.

Flores, M. C. (1992). *Bases para uma política militar.* Campinas: Editora da Unicamp.

Foessel, M. (2011). *Estado de vigilancia: crítica de la razón securitaria.* Madrid: Lengua de Trapo.

Fort, J. T. (2017). El fenómeno social del clientelismo en España. *Revista Internacional de Investigación en Ciencias Sociales, 13(1)*, 93-111.

Foucault, M. ((1975) 2006). Society must be defended. Translated by David Macey. *Lectures at the Collège de France, 1975-1976. Edited by Mauro Bertani and Alessandro Fontana.* New York: Picador.

Foucault, M. ((1978) 1991). Governmentality. In B. Graham, C. G., & P. M., *The Foucault Effect: Studies in Governmentality.* Chicago: University of Chicago Press.

Foucault, M. ((1978) 2007). Security, territory, population. Senellart, M. (Ed.). Translated by Graham Burchell. *Lectures at the Collège de France.* New York: Picador.

Foucault, M. ((1979) 2008). The birth of biopolitics. Senellart, M. (Ed.). Translated by Graham Burchell. *Lectures at the Collège de France.* New York: Picado.

Foucault, M. ((1984) 2019). *Power: The essential works of Michel Foucault 1954-1984.* London: Penguin UK.

Foucault, M. (1975). *Discipline and punish. Translated by Sheridan, A.* Paris: Gallimard.

Foucault, M. (1978). *The history of sexuality. Translated by Robert Hurley.* New York: Pantheon.

Franz, K. ((1925) 2015). *The Trial.* London: Xist Publishing.

Fuchs, C. (2011). Web 2.0, prosumption, and surveillance. *Surveillance & Society, 8(3)*, 288-309.

Fukuyama, F. (1989). The end of history? *The national interest, (16),* 3-18.

Gandy Jr, O. H. (2012). Statistical surveillance. In K. Ball, D. Lyon, & K. D. Haggerty, *Handbook of surveillance studies* (p. 125). London: Routledge .

Ganesh, S. (2016). Digital age - managing surveillance: Surveillant individualism in an era of relentless visibility. *International Journal of Communication, 10.*, 14-27.

Ganor, B. (2011). *The counter-terrorism puzzle: A guide for decision makers.* New Brunswick: Transaction Publishers.

Garcia, F. G., Vieira, A., & Mendes, B. (2014). *Teoria da história em debate: Modernidade, narrativa, interdisciplinaridade.* Belo Horizonte: Paco.

García, P., & Tauste, A. M. (2006). Sexo, política y subversión. El chiste popular en la época franquista. *Círculo de lingüística aplicada a la comunicación, (27), 1*, http://hispadoc.es/servlet/articulo?codigo=2122966.

Garthoff, R. L. (2004). Foreign intelligence and the historiography of the Cold War . *Journal of Cold War Studies, 6(2)*, 21-56.

Gaspari, E. (2014). *A ditadura envergonhada.* Rio de Janeiro: Editora Intrínseca.

Gaspari, E. (2014). *A ditadura escancarada.* Rio de Janeiro: Editora Intrínseca.

George, A. (2002). *The epic of Gilgamesh: the Babylonian epic poem and other texts in Akkadian and Sumerian.* London: Penguin.

Gilabert, F. J. (2013). Democracia 4.0: Desrepresentación en el voto telemático de las leyes. *Revista Internacional de Pensamiento Político, 8*, 119-138.

Gill, P. (2003). Democratic and parliamentary accountability of intelligence services after September 11th. *Geneva Centre for the Democratic control of Armed Forces (DCAF)* (pp. 1-25). Geneva: DCAF Working Papers.

Gill, P. (2016). *Intelligence governance and democratisation: A comparative analysis of the limits of reform.* London: Routledge.

Gill, P., & Phythian, M. (2016). What is intelligence studies? . *The International Journal of Intelligence, Security, and Public Affairs, 18(1)*, 5-19.

Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world.* Medford, MA: John Wiley & Sons.

Glondys, O. (2012). *La guerra fría cultural y el exilio republicano español: Cuadernos del Congreso por la Libertad de la Cultura, 1953-1965.* Madrid: Consejo Superior de Investigaciones Científicas.

Gonçalves, J. B. (2008). *Sed quis custodiet ipso custodes? o controle da atividade de inteligência em regimes democráticos: os casos de Brasil e Canadá.* Brasilia: Doctoral dissertation, Universidade de Brasilia.

Gonçalves, J. B. (2010). *Políticos e espiões: o controle da atividade de inteligência.* Niterói: Impetus.

González Cussac, J. L., Hinojar, B. L., & Hernández, A. F. (2012). *Servicios de inteligencia y Estado de Derecho.* Valencia: Tirant lo Blanch.

González Hernández, A. (2018). *Una visión panorámica del SITEL: fundamentos técnicos y jurídicos.* Salamanca: Trabajo de Fin de Grado en Derecho Administrativo, Universidad de Salamanca.

González, M. C. (2019). ¿Proteger o premiar al whistleblower?: un debate pendiente en España. In Bernal, J. S.; Del Teso, A. E. & García, N. R. *Corrupción: compliance, represión y recuperación de activos*, 431-448. Valencia: Tirant lo Blanch.

Gordon, D. R. (1987). The electronic panopticon: A case study of the development of the National Criminal Records System. *Politics & Society, 15(4)*, 483-511.

Gray, R., Owen, D., & Adams, C. (1996). *Accounting & accountability: Changes and challenges in corporate social and environmental reporting.* London: Prentice Hall.

Guasch Portas, V., Fuensanta, S., & Ramón, J. (2015). El interés legítimo en la protección de datos. *RDUNED: revista de derecho UNED, 16,* 417-438.

Guinan, J., & O'Neill, M. (2018). The institutional turn: Labour's new political economy. *Renewal: a Journal of Labour Politics, 26(2)*, 5-16.

Guldi, J., & Armitage, D. (2014). *The history manifesto*. Cambridge: Cambridge University Press.

Gulyás, Á. (2016). Social Media and Journalism: Hybridity, convergence, changing relationship with the audience, and fragmentation. In B. Franklin, & S. (. Eldridge II, *The Routledge companion to digital journalism studies* (pp. 396-406). London: Routledge.

Gumbrecht, H. U. (2004). *Production of presence: What meaning cannot convey.* Stanford: Stanford University Press.

Gumbrecht, H. U. (2014). *Our broad present: Time and contemporary culture.* New York: Columbia University Press.

Gürses, S., Troncoso, C., & Diaz, C. (2011). *Engineering privacy by design.* Leuven: K.U. Leuven/IBBT.

Habermas, J. ((1991) 2015). *Between facts and norms: Contributions to a discourse theory of law and democracy.* Philadelphia, PA: John Wiley & Sons.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British journal of sociology, 51(4)*, 605-622.

Hahn, R. W., & Wallsten, S. (2006). The economics of net neutrality. *The Economists' Voice, 3(6)*.

Hall, S. (2001). Encoding/decoding. *Media and cultural studies: Keyworks, 2*.

Hameleers, M., & Schmuck, D. (2017). It's us against them: A comparative experiment on the effects of populist messages communicated via social media. *Information, Communication & Society, 20(9)*, 1425-1444.

Hamilton, A., Madison, J., & Jay, J. (2008). *The federalist papers.* Oxford: Oxford University Press.

Han, B. C. (2015). *The transparency society.* Stanford: Stanford University Press.

Han, B. C. (2017). *The scent of time: A philosophical essay on the art of lingering.* New York: John Wiley & Sons.

Hands, J. (2007). Between agonistic and deliberative politics: towards a radical e-democracy. In Dahlberg, L. & Siapera, E., *Radical Democracy and the Internet: Interrogating Theory and Practice* (pp. 89-107). New York: Palgrave Macmillan.

Hardt, M., & Negri, A. (2004). *Multitud: guerra y democracia en la era del Imperio.* Madrid: Editorial Debate.

Hardt, M., & Negri, A. (2009). *Commonwealth.* Cambridge, MA: Belknap Press.

Haucap, J., & Heimeshoff, U. (2014). Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization? *International Economics and Economic Policy, 11(1-2)*, 49-61.

Hayez, P. (2011). National oversight of international intelligence cooperation. In H. Born, I. Leigh, & A. Wills, *International Intelligence Cooperation and Accountability* (pp. 163-181). London: Routledge.

Headley, A., & Garcia-Zamor, J. C. (2014). The privatization of prisons and its impact on transparency and accountability in relation to maladministration. *International Journal of Humanities, Social Sciences and Education, 1(8),*, 23-34.

Herman, M. (2013). *Intelligence services in the information age.* London: Routledge.

Hester, H. (2018). *Xenofeminism.* New York: John Wiley & Sons.

Heywood, A. (2016). *Introducción a la teoría política.* Valencia: Tirant lo blanch.

Hier, S. P. (2003). Hier, Sean P. (2003). "Probing the SurveillantAssemblage: on the dialectics of surveillance practices as processes of social control. *Surveillance & Society, 1(3)*, 399-411.

Higgins, P., Short, D., & South, N. (2013). Protecting the planet: a proposal for a law of ecocide. *Crime, Law and Social Change, 59(3)*, 251-266.

Hiltz, S. R., & Turoff, M. (1987). *The network nation: Human communication via computer*. Cambridge, MA: Addison-Wesley.

Hobbes, T. ((1650) 2010). *The elements of law, natural and politic.* Whitefish: Kessinger Publishing.

Hobbes, T. ((1651) 2016). *Leviathan (Longman Library of Primary Sources in Philosophy).* London: Routledge.

Holmes, S. M., & Castañeda, H. (2016). Representing the European refugee crisis in Germany and beyond: Deservingness and difference, life and death. *American Ethnologist 43, no. 1.*, 12-24.

Horkheimer, M., & Adorno, T. W. ((1947) 1972). *Dialectic of Enlightenment.* New York: Seabury Press.

Howard, M. (1978). *War and the liberal conscience.* Oxford: Oxford university press.

Hristova, S. (2014). Visual memes as neutralizers of political dissent. *tripleC: Communication, Capitalism & Critique*, 12(1), 265-276.

Hu, Y., Shin, J., & Tang, Z. (2010). Pricing of online advertising: cost-per-click-through vs. cost-per-action. *43rd Hawaii International Conference on System Sciences* (pp. 1-9). IEEE.

Hunter, W. (1997). *Eroding military influence in Brazil: Politicians against soldiers.* Chapel Hill: The University of North Carolina Press.

Huxley, A. ((1932) 1998). *Brave New World.* London: Vintage.

Iaconesi, S. (2017). Interface and data biopolitics in the age of hyperconnectivity. Implications for design. *The Design Journal*, *20*(sup1), S3935-S3944.

Immergut, E. M. (2006). Historical institutionalism in political science and the problem of change. In Mahoney, J.; Wimmer, A., & Kossler, R., *Understanding Change* (pp. 237-259). London: Palgrave Macmillan.

Iser, W. (2002). Os atos de fingir ou o que é fictício no texto ficcional. *Teoria da literatura em suas fontes, 2*, 955-987.

Jandrić, P., Ryberg, T., Knox, J., Lacković, N., Hayes, S., Suoranta, J., & Ford, D. R. (2019). Postdigital dialogue. *Postdigital Science and Education*, 1(1), 163-189.

Joas, H. (1996). *The creativity of action.* Chicago: University of Chicago Press.

Joffily, M. R. (2013). *No centro da engrenagem. Os interrogatórios na Operação Bandeirante e no DOI de São Paulo (1969-1975).* Sao Paulo: Doctoral dissertation, Universidade de São Paulo.

Joffily, M. R. (2019). Documentos dos EUA referentes às ditaduras do Cone Sul: desafios metodológicos. *Revista Eletrônica da ANPHLAC, (25),* 275-302.

Johns, F. (2005). Guantanamo Bay and the Annihilation of the Exception. *European Journal of International Law, 16(4)*, 613-635.

Johnson, D., & Regan, P. (2014). *Transparency and surveillance as sociotechnical accountability: A house of mirrors.* London: Routledge.

Johnston, R. (2005). Analytic culture in the US intelligence community. *An ethnographic study (No. 14). Central Intelligence Agency.*

Jordan, T. (2007). Online direct action: Hacktivism and radical democracy. In Dahlberg, L. & Siapera, E. *Radical democracy and the internet*, 73-88. London: Palgrave Macmillan UK.

Kant, I. ((1781) 1998). *Critique of pure reason.* Translated and edited by Guyer, P. & Wood, A. Cambridge: Cambridge University Press.

Kant, I. ((1798) 1974). *Anthropology from a pragmatic point of view.* Translated Gregor, Mary J. The Hague: Martinus Nijhoff.

Kaplan, M. (2018). Spying for the people: surveillance, democracy and the impasse of cynical reason. *JOMEC Journal*, (12), 166-190.

Karatani, K. (2005). *Transcritique: On Kant and Marx.* Cambridge, MA: MIT Press.

Kearney, A. T. (2014). Rethinking personal data: A new lens for strengthening trust. *World Economic Forum.*

Kent, S. ((1949) 2015). *Strategic intelligence for American world policy.* Princeton: Princeton University Press.

Kersting, W. (1992). Kant's Concept of the State. *Essays on Kant's Political Philosophy.*, 143-165.

Khan, L. M. (2016). Amazon's antitrust paradox. *Yale lJ, 126*, 710.

Khan, L. M., & Vaheesan, S. (2017). Market power and inequality: The antitrust counterrevolution and its discontents. *Harvard Law and Policy Review, 11*, 235.

Klingemann, H. D., & Fuchs, D. (1998). Citizens and the state: a relationship transformed. *Beliefs in government, 1.*

Knorr, K. E. (1964). Foreign intelligence and the social sciences. *Center of International Studies, Woodrow Wilson School of Public and International Affairs, Princeton University.*

Koppell, J. G. (2010). *World rule: Accountability, legitimacy, and the design of globalgovernance.* Chicago: University of Chicago Press.

Koselleck, R. (2004). *Futures past: on the semantics of historical time.* New York: Columbia University Press.

Kucinski, B., & Tronca, I. (2013). *Pau de arara: a violência militar no Brasil: com apêndices documentais.* Sao Paulo: Fundação Perseu Abramo.

Laclau, E. (2008). *On populist reason.* New York: Verso.

Land, N. (2017). *A quick-and-dirty introduction to accelerationism.* Retrieved from https://jacobitemag.com/2017/05/25/a-quick-and-dirty-introduction-to-accelerationism/ Jacobite, consulted in 13/03/2020.

Lang, B. (1991). *Writing and the moral self.* London: Routledge.

Lee, A., & King, F. D. (2015). From text, to myth, to meme: Penny Dreadful and Adaptation. *Cahiers victoriens et édouardiens*, 82.

Leite, G. S., & Lemos, R. (2014). *Marco civil da internet.* Sao Paulo: Editora Atlas SA.

Lemieux, F. (2018). Intelligence and surveillance technologies. In Lemieux, F. *Intelligence and State Surveillance in Modern Societies*, 165-190. Bingley: Emerald Publishing Limited.

Lenza, P. (2010). *Direito constitucional esquematizado: igualdade formal e material.* São Paulo: Saraiva.

Lerner, J., & Triole, J. (2002). Some simple economics of open source. *Journal of Industrial Economics, 52*, 197-234.

Levy, C. (2010). Refugees, Europe, camps/state of exception: “into the zone”, the European Union and extraterritorial processing of migrants, refugees, and asylum-seekers (theories and practice). *Refugee Survey Quarterly 29, no. 1*, 92-119.

Levy, S. (1994). *Hackers. Heroes of the computer revolution.* New York: Dell Publishing.

Linz, J. J. (1981). *Informe sociológico sobre el cambio político en España, 1975-1981: IV informe FOESSA.* Madrid: Euramérica.

Lobo-Guerrero, L. (2007). Biopolitics of specialized risk: an analysis of kidnap and ransom insurance. *Security Dialogue, 38(3)*, 315-334.

Locke, J. ((1689) 2012). *A letter concerning toleration.* Washington D.C.: Springer Science & Business Media.

Lowenthal, M. M. (1993). Intelligence epistemology: Dealing with the unbelievable. *International Journal of Intelligence and Counter Intelligence, 6(3)*, 319-325.

Luckhurst, R. (2013). *The trauma question.* London: Routledge.

Luhmann, N. ((1999) 2012). *Theory of society.* Stanford, CA: Stanford University Press.

Luhmann, N. (1986). The autopoiesis of social systems. *Sociocybernetic paradoxes, 6(2).*, 172-192.

Luhmann, N. (2013). *A sociological theory of law.* London: Routledge.

Lukács, G. (1969). *Historia y conciencia de clase; estudios de dialéctica marxista.* México DF: Grijalbo Imprenta.

Lustgarten, L. (2004). National security, terrorism and constitutional balance. *The Political Quarterly, 75(1)*, 4-16.

Lynn, B. C. (2009). *Cornered: The new monopoly capitalism and the economics of destruction.* New York: John Wiley & Sons.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society.* Minneapolis: Univeristy of Minnesota Press.

Lyon, D. (2002). Surveillance studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society, 1(1)*, 1-7.

Lyon, D. (2006). *Theorizing surveillance.* London: Routledge.

Lyon, D. (2007). *Surveillance studies: An overview.* Cambridge: Polity Press.

Lyon, D. (2014). Surveillance and the eye of God. *Studies in Christian Ethics, 27(1)*, 21-32.

MacFarlane, S. N., & Khong, Y. F. (2006). *Human security and the UN: A critical history.* Bloomington: Indiana University Press.

Machiavelli, N. ((1532) 1996). *Discourses on Livy,* translated by Harvey, C. M. & Nathan, T. Chicago: University of Chicago Press.

Malcolm, J. (2008). *Multi-stakeholder governance and the Internet Governance Forum.* Sydney: Terminus Press.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & society, 1(3),* 331-355.

Margolis, M. and Resnick, D. (2000). *Politics as Usual: The Cyberspace 'Revolution'*. Thousand Oaks, CA: Sage.

Marinoni, B. (2015). Concentração dos meios de comunicação de massa e o desafio da democratização da mídia no Brasil. *Análise, 13*, 1-28.

Marques, V. B. (2017). The dissidence of one with oneself: Lying in Vladimir Jankélévitch. *From Kierkegaard to Heidegger: 2nd Workshop of the project Experimentation and Dissidence.* Lisbon: University of Lisbon.

Marsh, D., & Smith, M. (2000). Understanding policy networks: towards a dialectical approach. *Political studies, 48(1)*, 4-21.

Martin, A. K., Van Brakel, R., & Bernhard, D. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society 6(3)*, 213-232.

Martínez Cabezudo, F. (2014). *Copyright y copylef. Modelos para la ecología de los saberes.* Sevilla: Aconcagua Libros

Marvin, H. (1977). *Cannibals and Kings. The origins of culture.* New York: Random House Inc.

Marx, G. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of social issues, 59(2)*, 369-390.

Marx, G. (2004). Some concepts that may be useful in understanding the myriad forms and contexts of surveillance. *Intelligence & National Security, 19(2)*, 226-248.

Marx, G. T. (2009). A tack in the shoe and taking off the shoe neutralization and counter-neutralization dynamics. *Surveillance & Society, 6(3),* 294-306.

Mashaw, J. L. (2006). Accountability and institutional design: Some thoughts on the grammar of governance. *Public Law Working Paper, (116)*, 115-156.

Matei, F. C. (2014). The media's role in intelligence democratization. *International Journal of Intelligence and CounterIntelligence, 27(1)*, 73-108.

Matey, G. D. (2010). The development of intelligence studies in Spain. *International Journal of Intelligence and Counterintelligence, 23(4)*, 748-765.

Matey, G. D., & Guisado, Á. C. (2019). Los secretos oficiales en España: un dilema entre transparencia y seguridad nacional. *Gladius et Scientia. Revista de Seguridad del CESEG, (1)*.

Mathiesen, T. (1997). The viewer society: Michel Foucault's Panopticon'revisited. *Theoretical criminology, 1(2)*, 215-234.

Matos, A.S. de M.C., & Collado, F. G. (2020). *Más allá de la biopolítica: biopotencia, bioarztquía, bioemergencia*. Girona: Documenta Universitaria.

McAdam, D., Tarrow, S., & Tilly, C. (2003). Dynamics of contention. *Social Movement Studies, 2(1)*, 99-102.

McGrath, J. E. (2004). *Loving Big Brother: Performance, privacy and surveillance space.* Chicago: Psychology Press.

McNay, L. (1994). *Foucault.* Polity: Cambridge.

Mechi, P. (2015). A Guerrilha do Araguaia e a repressão contra camponeses: reflexões sobre os fundamentos e as práticas repressivas do estado brasileiro em tempos de ditadura. *História Revista, 20(1),* 48-70.

Milgram, S. (1974). *Obedience to authority: An experimental view*. New York: HarperCollins

Monk, B. M. (2017). *Tor, what is it good for? How crime predicts domain failure on the darkweb* . Doctoral dissertation, Arts & Social Sciences: School of Criminology, SFU University.

Monteiro, R. L. (2014). The balance between freedom and security in the age of surveillance: A brief analysis of the recent intelligent electronic surveillance scandals. *Available at SSRN 2468060.*

Moore, M., & Tambini, D. (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple.* Oxford: Oxford University Press.

Morales, R. M. (1999). El principio constitucional de intervención indiciaria. *Revista de la Facultad de Derecho de la Universidad de Granada, (2)*, 341-506.

Moran, P. (2007). *Virginia Woolf, Jean Rhys, and the aesthetics of trauma.* New York: Palgrave Macmillan.

Moreira, S. V. (2015). *Indústria da comunicação no Brasil: dinâmicas da academia e do mercado.* Rio de Janeiro: UERJ Editorial.

Moretón Toquero, M. (2014). Los límites del derecho de acceso a la información pública. *Revista jurídica de Castilla y León, (33)*, 121-145.

Morozov, E. (2013). *To save everything, click here: Technology, solutionism, and the urge to fix problems that don't exist.* Londres: Penguin.

Motta, R. P. (2014). A ditadura nas universidades: repressão, modernização e acomodação. . *Ciência e Cultura, 66(4)*, 21-26.

Muñoz Cáliz, B. (2005). *El teatro crítico español durante el franquismo, visto por sus censores.* Alcalá de Henares: Universidad de Alcalá.

Murua, I. (2017). No more bullets for ETA: The loss of internal support as a key factor in the end of the Basque group's campaign. *Critical Studies on Terrorism, 10(1)*, 93-114.

Neuschäfer, H. J. (1994). *Adiós a la España eterna: la dialéctica de la censura: novela, teatro y cine bajo el franquismo.* Madrid: Anthropos Editorial.

New, W. H. (2003). *A history of Canadian literature.* Montreal: McGill-Queen's Press-MQUP.

Noam, E. (2002). Why the Internet Is Bad for Democracy. *Communications of the ACM*, 48(10), 57–58.

Numeriano, C. R. (2007). *A inteligência civil do Brasil, Portugal e Espanha: Legados tários como constrangimentos à democratização da inteligência de estado na transição e consolidação democrática.* Recife: Thesis Dissertation, Universidade Federal de Pernambuco.

O'Donnell, G. (1998). Horizontal accountability in new democracies. *Journal of demo-cracy, 9 (3)*, 112-126.

Oliveira, L. (2011). Ditadura militar, tortura e história: A" vitória simbólica" dos vencidos. . *Revista Brasileira de Ciências Sociais, 26(75),* 07-25.

Orwell, G. ((1949) 2009). *Nineteen eighty-four.* London: Everyman's Library.

Paine, T. ((1791) 2011). *Rights of man.* Calgary: Broadview Press.

Palacios, J. (2001). *23-F: El golpe del CESID.* Madrid: Planeta.

Pangrazio, L., & Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society, 21(2)*, 419-437.

Parsons, C. (2019). The (in) effectiveness of voluntarily produced transparency reports. *Business & Society, 58(1)*, 103-131.

Pascual, M. I. (2014). EL TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland . *Revista de Derecho Comunitario Europeo, 18(49)*, 943-971.

Patton, P. (1994). Metamorpho-logic: Bodies and powers in A Thousand Plateaus. *Journal of the British Society for Phenomenology, 25(2)*, 157-169.

Pavan, E. (2012). *Frames and connections in the governance of global communications: A network study of the Internet Governance Forum.* London: Lexington Books.

Payne, S. G. (2011). *The Franco Regime, 1936–1975.* Madison: University of Wisconsin Press.

Peñaranda, A. J. (2005). Los servicios de inteligencia en la transición. *Arbor CLXXX, 709*, 99-119.

Pereira, M. H. (2015). Nova direita? Guerras de memória em tempos de Comissão da Verdade (2012-2014). *Varia Historia, 31(57),* , 863-902.

Pérez, R. (2013). Repensando la memoria pública. *Conexión, (2)*, 54-75.

Pérez-Villalobos, M. C. (2002). *Derechos fundamentales y servicios de inteligencia.* Granada: Grupo Editorial Universitario.

Peters, M. A. (2004). Performative, performativity and the culture of performance: Knowledge management in the new economy. *Management in Education, 18(1)*, 35-38.

Peters, M. A., & Besley, T. (2019). Critical philosophy of the postdigital. *Postdigital Science and Education*, 1(1), 29-42.

Petersen, S. M. (2008). Loser generated content: From participation to exploitation. *First Monday, 13(3)*.

Petersen, M. B., & Laustsen, L. (2020). Dominant leaders and the political psychology of followership. *Current opinion in psychology*, (33), 136-141.

Pierson, P., & Skocpol, T. (2002). Historical institutionalism in contemporary political science. *Political science: The state of the discipline,* (3), 693-721.

Piketty, T. (2014). *Capital in the twenty-first century.* Cambridge, MA: Belknap Press.

Piketty, T., & Saez, E. (2013). Optimal labor income taxation. In A. J. Auerbach, R. Chetty, & e. al, *Handbook of public economics*, 391-474. Oxford: Elsevier.

Piñar Mañas, J. L. (2003). El derecho a la protección de Datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. *Cuadernos de Derecho Público, (19-20)*, 61-66.

Polanyi, K. (1944). *The great transformation.* Boston: Beacon press.

Poster, M. (1990). Foucault and Data Bases. *Discourse, 12(2),* 110-127.

Priego, E. (2016). Signal, not solution: Notes on why Sci-Hub is not opening access. *The winnower, 3*, e145624.

Prozorov, S. (2005). X/Xs: Toward a general theory of the exception. *Alternatives: Global, Local, Political, 30*, 82-97.

Purzycki, B., Apicella, C., & Atkinson, Q. e. (2016). Moralistic gods, supernatural punishment and the expansion of human sociality. *Nature 530. Retrieved from: https://doi.org/10.1038/nature16980*, 327–330.

Raab, C. (2013). *Increasing resilience in surveillance societies, IRISS project.* Edinburgh: The University of Edinburgh.

Raab, C. D., Jones, R., & Székely, I. (2015). Surveillance and resilience in theory and practice. *Media and Communication, 3(2)*.

Ramió, C. (2019). *Inteligencia artificial y administración pública: robots y humanos compartiendo el servicio público*. Madrid: Catarata.

Ramos, P. H. (2014). Towards a developmental framework for net neutrality: The rise of sponsored data plans in developing countries. *TPRC Conference Paper.*

Rancière, J. (1999). *Disagreement: Politics and philosophy.* Minneapolis: University of Minnesota Press.

Rancière, J. (2009). Contemporary art and the politics of aesthetics. In B. Hinderliter, & V. Maimon, *Communities of sense: Rethinking aesthetics and politics*, 31-50. Durham: Duke University Press Books.

Rancière, J. (2011). *The emancipated spectator.* London: Verso.

Rancière, J. (2015). *Dissensus: On politics and aesthetics.* London: Bloomsbury Publishing.

Rego, J. D. (1984). *Cooperativismo nacional: dimensões políticas econômicas.* Sao Paulo: Organização das Cooperativas Brasileiras.

Revenga Sánchez, M. (2001). Servicios de inteligencia y derecho a la intimidad. *Revista Española de Derecho Constitucional, 21, n. 61.*, 61-ss.

Revenga Sánchez, M. (2003). El control del Centro Nacional de Inteligencia - A males extremos, paliativos,. *Claves de Razón Práctica, n. 130*, 36-ss.

Rhodes, R. A. (1997). *Understanding governance: Policy networks, governance, reflexivity and accountability.* London: Open University.

Roberts, A. (2012). WikiLeaks: the illusion of transparency. *International review of administrative sciences, 78(1)*, 116-133.

Rodríguez, L. Z. (2014). *El tipo penal de tortura en la legislación española, a la luz de la jurisprudencia nacional e internacional.* Salamanca: Ediciones Universidad de Salamanca.

Rorty, R. ((1979) 2009). *Philosophy and the mirror of nature.* New Jersey: Princeton University Press.

Rorty, R. (1989). *Contingency, irony, and solidarity.* Cambridge: Cambridge University Press.

Rosa Camacho, I. (2004). *El vano ayer.* Madrid: Planeta.

Roth-Isigkeit, D. (2018). *The plurality trilemma: A geometry of global legal thought.* London: Springer.

Rubinstein, I. S., & Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Tech. LJ, (28)*, 1333.

Ruiz Miguel, C. (2005). El CESID: Historia de un intento de modernización de los servicios de Inteligencia. *Arbor CLXXX, 709*, 121-150.

Rüsen, J. (2005). *History: Narration, interpretation, orientation.* New York: Berghahn Books.

Saad-Filho, A. (2013). Mass protests under 'left neoliberalism': Brazil, June-July 2013. *Critical Sociology, 39(5)*, 657-669.

Sagers, C. L. (2014). *Examples & explanations for antitrust.* New York: Wolters Kluwer Law & Business.

Sain, M. (1999). *Democracia e inteligencia de Estado en la Argentina.* Buenos Aires: Mimeo.

Sainz Varela, J. A. (2018). *Secreto de archivo acceso a los documentos públicos, transparencia y otras manías de archivero.* Vitoria-Gasteiz: Real Sociedad Bascongada de Amigos del País.

Salter, M. B. (2008). *Politics at the Airport.* Minneapolis: University of Minnesota Press.

San Martín, J. I. (1984). *Servicio especial: a las oŕdenes de Carrero Blanco, de Castellana a El Aaiún.* Madrid: Planeta.

Santamaría García, A. (2019). Regiones, subalternos, invisibles, cultura política y desigualdad. Crisis y retorno de lo social en la historia de América Latina en el siglo XX. *Revista de El Colegio de San Luis, 9(18)*, 285-326.

Santamaria Guinot, L. (2017). Identidad emocional y tertulias televisivas en el contexto político de Catalunya. . *Zer: Revista de Estudios de Comunicacion, 22(43)*, 129-147.

Sarkis, O., & Novais, L. A. (1994). *O SNI nas pegadas do PT.* Sao Paulo: Revista Isto É.

Schaar, P. (2010). Privacy by design. *Identity in the Information Society, 3(2)*, 267-274.

Schafer, V., Musiani, F., & Le Crosnier, H. (2014). Net Neutrality: an issue of democracy. *Transforming Politics and Policy in the Digital Age. IGI Global.*, 22-38.

Scharpf, F. W. (1997). Games real actors play. Actor-centered institutionalism. *Policy research, 55.*

Schedler, A., Diamond, L. J., & Plattner, M. F. (1999). *The self-restraining state: power and accountability in new democracies.* Boulder, CO: Lynne Rienner Publishers.

Scheinin, M., & Vermeulen, M. (2011). International law: Human rights law and state responsibility. In Born, H.; Leigh, I. & Wills, A. *International Intelligence Cooperation and Accountability* (pp. 264-286). London: Routledge.

Schlembach, R. (2016). *Against old Europe: critical theory and alter-globalization movements.* London: Routledge.

Schmitt, C. ((1922) 1985). *Political theology.* Translated by George Schwab. Cambridge, MA: MIT Press.

Schmitt, C. ((1932) 1976). *The concept of the political.* Translated by George Schwab. New Jersey: Rutgers University Press.

Schmitt, C. ((1934) 2008). *Political theology II.* Translated by Michael Hoelzl and Graham Ward. Cambridge: Polity.

Schneider, V. (2005). *Policy-networks in a complex systems perspective. A new look on an old data set.* Baden-Wrttemberg, Germany: University of Constance.

Sen, S., Giesel, M. E., Gold, R., & Hecht, B. (2015). Turkers, scholars,"Arafat" and "peace": Cultural communities and algorithmic gold standards. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 826-838. ACM.

Shattuck, J. (1984). Computer matching is a serious threat to individual rights. . *Communications of the ACM, 27(6),* 538-541.

Shulsky, A. N., & Schmitt, G. J. (2002). *Silent warfare: understanding the world of intelligence.* Washington, DC: Potomac Books Inc.

Silva, G. E., Bergmann, H., & Marques, R. M. (2019). False perception of gratuity: Zero-rating practice and the Civil Rights Framework for the Internet. *Transinformação, 31*, https://doi.org/10.1590/2318-0889201931e180021 .

Simili, I. G. (2014). Memórias da dor e do luto: as indumentárias político-religiosas de Zuzu Angel. *Revista Brasileira de História das Religiões, 6(18)*, 165-182.

Simon, B. (2005). The return of panopticism: Supervision, subjection and the new surveillance. *Surveillance & Society, 3(1)*, 15-27.

Singer, P. (2014). La economía solidaria en Brasil. La economía Popular y Solidaria. *El Ser Humano Sobre el Capital, 47*.

Sintomer, Y. (2018). From deliberative to radical democracy? Sortition and politics in the twenty-first century. *Politics & Society*, *46*(3), 337-357.

Sneed, P. (2008). Favela Utopias: The" Bailes Funk" in Rio's Crisis of Social Exclusion and Violence. *Latin American research review*, 57-79.

Soares, F. B., Recuero, R., & Zago, G. (2019). Asymmetric polarization on Twitter and the 2018 Brazilian presidential elections. *Proceedings of the 10th International Conference on Social Media and Society*, 67-76.

Soares, G. A., D'Araujo, M. C., & Castro, C. (1995). *A volta aos quartéis: a memória militar sobre a abertura.* Rio de Janeiro: Relume Dumará.

Soh, W. Y. (2020). Digital protest in Singapore: the pragmatics of political Internet memes. Media, Culture & Society. https://doi.org/10.1177/0163443720904603.

Solove, D. J. (2013). Privacy self-management and the consent paradox. *Harvard Law Review, 126(7),* 1-880.

Sphere Ramiro, M. (2011). Los cambios previstos en la Directiva 95/46/CE de protección de datos personales. *La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, (50)*.

Spivak, G. C. ((1988) 2016). *Can the subaltern speak?* London: Macat International Limited.

Srnicek, N. (2013). #Accelerate: Manifesto for an accelerationist politics. In Johnson J. (Ed.), *Dark Trajectories: Politics of the Outside*, 135-155. Miami: Name.

Starr, P. (2011). The Manichean World of Tim Wu. *The American Prospect*, 63-66.

Steiner, C. M. (1987). The seven sources of power: An alternative to authority. *Transactional analysis journal, 17(3)*, 102-104.

Steinmo, S. (2008). Historical institutionalism. In Della Porta, D. & Keating, M. (Eds.). *Approaches and methodologies in the social sciences: A pluralistic perspective* (pp. 118-138). Cambridge: Cambridge University Press.

Stiglitz, J. E. (1986). The new development economics. *World Development, 14(2)*, 257-265.

Stiglitz, J. E. (1994). Economic growth revisited. *Industrial and Corporate Change, 3(1)*, 65-110.

Stocker, B. (2006). *Routledge philosophy guidebook to Derrida on deconstruction.* London: Routledge.

Striphas, T. (2015). Algorithmic culture. *European Journal of Cultural Studies, 18(4-5)*, 395-412.

Sun, H. (2013). A longitudinal study of herd behavior in the adoption and continued use of technology. *Mis Quarterly*, 1013-1041.

Tatagiba, L., & Galvão, A. (2019). Las protestas en Brasil en época de crisis (2011-2016). *Opinião Pública, 25(1)*, 63-96.

Tay, C. (2019). *Whose life is it anyway? Identity, surveillance and power in the digital world.* Christchurch: University of Canterbury.

Taylor, M., Wells, G., Howell, G., & Raphael, B. (2012). The role of social media as psychological first aid as a support to community resilience building. *The Australian Journal of Emergency Management, 27(1),* 20-36.

Thin, N., Verma, R., & Uchida, Y. (2017). Culture, development and happiness. *Happiness, 260*.

Tilly, C., & Argilés, R. A. (2007). *Violencia colectiva.* Barcelona: Editorial Hacer.

Todorov, T. (2009). *Imperfect garden: The legacy of humanism.* New Jersey: Princeton University Press.

Toret, E., & Pérez de Lama, J. (2012). Devenir cyborg, era postmediática y máquinas tecnopolíticas. Guattari en la sociedad red. In Berti, G. (Ed). *Félix Guattari. Los ecos del pensar. Entre la filosofía, el arte y la clínica.* Barcelona: HakkaBooks.

Toret, J. (2012). *Una mirada tecnopolıtica sobre los primeros dıas del 15M.* Democracia Distribuida. Miradas de la Universidad Nómada al M, 15.

Trías, E. ((1982) 2011). *Lo bello y lo siniestro.* Barcelona: Debolsillo.

Tsuruta, T. (2008). Between moral economy and economy of affection. *Contemporary perspectives on African moral economy*, 35-52.

Turner, L. (2011). *Metamodernist Manifesto.* retrieved from http://metamodernism.org, consulted in 15/09/2020.

Tusell, J., Alted, A., & Mateos, A. (1990). *La oposición al régimen de Franco. Estado de la cuestión y metodología de la investigación.* Madrid: UNED.

Valero, F. M. (1997). *La escuela y el estado nuevo: la depuración del magisterio nacional, 1936-1943.* Madrid: Ambito Editores.

Van den Akker, R., Gibbons, A., & Vermeulen, T. (2017). *Metamodernism: Historicity, affect, and depth after postmodernism.* London: Rowman & Littlefield.

Van Dijk, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & society, 12(2)*, 197-208.

Vilar, P., & Gázquez, J. M. (1986). *La guerra civil española.* Barcelona: Crítica.

Villar Cirujano, E. (2015). *Espías entre el franquismo y la democracia: los informes confidenciales deServicio Central de Documentación (SECED) entre 1974 y 1977.* Madrid: Doctoral dissertation, Universidad Complutense de Madrid.

Virno, P. (2003). *A Grammar of the multitude.* Los Angeles: Semiotext.

Voĭnovich, V. ((1986) 1990). *Moscow 2042.* Boston: Mariner Books.

Wacquant, L. J. ((1999) 2009). *Prisons of poverty.* Minneapolis: University of Minnesota Press.

Walzer, M. ((1983) 2008). *Spheres of justice: A defense of pluralism and equality.* London: Basic Books.

Weber, M. (1978). Economy and society: An outline of interpretive sociology. Los Angeles: University of California Press.

Weems, S. (2014). *Ha!: The science of when we laugh and why.* New York: Basic Books.

Weiss, T. G. (2016). *Humanitarian intervention.* New York: John Wiley & Sons.

Westerfield, H. B. (1996). America and the world of intelligence liaison. *Intelligence and National Security, 11(3)*, 523-560.

White, G., & Ariyachandra, T. (2016). Big Data and ethics: examining the grey areas of big data analytics. *Issues in Information Systems*, 17(4).

White, H. (2014). *The practical past (Vol. 17).* Chicago: Northwestern University Press.

Whitson, J. R. (2013). Gaming the quantified self. *Surveillance & Society, 11(1/2)*, 163-176.

Wieringa, M. (2020). What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 1-18.

Wilde, O. ((1905) 2010). *De Profundis.* London: Modern Library.

Wilhelm, A. (2002). When Everything Is Intelligence – Nothing Is Intelligence . *Occasional Papers, 1 (4). Sherman Kent Center for Intelligence Analysis.*

Williams, L. (2009). Haraway contra Deleuze and Guattari: The question of the animals. *Communication, Politics & Culture, 42(1)*, 42.

Wills, A. (2012). Financial oversight of intelligence services. In H. Born, & A. Wills, *Overseeing Intelligence Services* (pp. 151-180). Geneva: DCAF.

Wood, D. M. (2007). Beyond the panopticon? Foucault and surveillance studies. *Space, knowledge and power: Foucault and geography*, 245-263.

Wood, D., Ball, K. S., Lyon, D., Norris, C., & Raab, C. D. (2006). *Information commissioner's report to parliament on the state of surveillance.* London: Information Commissioner's Office.

Wright, A. (2011). Fit for purpose? Accountability challenges and paradoxes of domestic inquiries. In Born, H. Leigh, I. & Wills, A. *International Intelligence Cooperation and Accountability*, 182-210. London: Routledge.

Wu, T. (2010). *The master switch: The rise and fall of information empires.* London: Vintage.

Yang, G., & Jiang, M. (2015). The networked practice of online political satire in China: Between ritual and resistance. *International Communication Gazette*, 77(3), 215-231.

Yar, M. (2003). Panoptic Power and the Pathologisation of Vision: Critical Reflections on the Foucauldian Thesis. *Surveillance & Society, 1(3)*, 254-271.

Yauri-Miranda, J. R. (2018). Securitization as a process of managing and producing risks. Between normality and political exceptionality in security. *Revista Española de Ciencia Política-RECP, (46)*, 231-256.

Yauri-Miranda, J. R. (2019). Militarización y legalismo en la gestión policial de la criminalidad en Brasil. *Estado, Gobierno y Gestión Pública, (32)*, 127-149.

Yin, R. K. (1989). Case study research: Design and methods, revised edition. *Applied Social Research Methods Series, 5.*

Yin, R. K. (1994). *Case study research: Design and methods .* Newbury Park, CA: SAGE Publications.

Zaverucha, J. (1994). *Rumor de sabres: controle civil ou tutela militar? Estudo comparativo das transições democráticas no Brasil, na Argentina e na Espanha.* Sao Paulo: Editora Atica.

Zaverucha, J. (2008). De FHC a Lula: A militarização da Agência Brasileira de Inteligência. *Revista de Sociologia e Política. Curitiba, v. 16*, 177-195.

Zedner, L. (2003). Too much security? *International journal of the sociology of law, 31(3)*, 155-184.

Zegart, A. B. (2000). *Flawed by design: The evolution of the CIA, JCS, and NSC.* Redwood City: Stanford University Press.

Zorzo Ferrer, F. J. (2005). Historia de los servicios de inteligencia: El periodo predemocrático. *ArborCLXXX, 709*, 75-98.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* London: Public Affairs.

Appendices

Annex I

Control Commission of Credits Intended For Reserved Funds. List of Parliament Initiatives in each legislature (in Spanish).

VI Legislatura (1996-2000) Iniciativas encontradas 0

VII Legislatura (2000-2004) Iniciativas encontradas 0

VIII Legislatura (2004-2008) Iniciativas encontradas 29

Convergencia i Unio (18/05/2004, Director CNI, explicar trabajo desarrollado, caducado), ERC (14/07/2004, Director CNI, explicar si CNI afectó actividades ERC y Eusko Alkartasuna, caducado), Gobierno (04/10/2004, Ministros Exteriores, Interior, Defensa, justificar uso de créditos reservados), PP (29/03/2005, Director CNI, relación del centro con un miembro del PSOE, rechazado), Grupo Parlamentario de Izquierda Verde-Izquierda Unida-Iniciativa per Catalunya Verds (07/11/2005, Director CNI, explicar vuelos de la CIA en Mallorca, rechazado), Grupo Parlamentario de Izquierda Verde-Izquierda Unida-Iniciativa per Catalunya Verds (07/11/2005, Ministro Interior, explicar vuelos de la CIA en Mallorca, rechazado), Coalición Canaria (16/11/2005, Ministro de Interior, explicar vuelos de la CIA en España, rechazado), Coalición Canaria (16/11/2005, Director CNI, explicar vuelos de la CIA en España, rechazado), Grupo Parlamentario de Izquierda Verde-Izquierda Unida-Iniciativa per Catalunya Verds (25/11/2005, Director CNI, explicar vuelos de la CIA en España, rechazado), Grupo Parlamentario de Izquierda Verde-Izquierda Unida-Iniciativa per Catalunya Verds (25/11/2005, Ministro Interior, explicar vuelos de la CIA en España, rechazado), Grupo Parlamentario de Izquierda Verde-Izquierda Unida-Iniciativa per Catalunya Verds (25/11/2005, Ministro Defensa, explicar vuelos de la CIA en España, rechazado), Coalición Canaria (25/11/2005, Director CNI, explicar vuelos de la CIA en España, rechazado), Coalición Canaria (25/11/2005, Ministro Interior, explicar vuelos de la CIA en España, rechazado), Grupo Parlamentario de Izquierda Verde-Izquierda Unida-Iniciativa per Catalunya Verds (27/01/2006, Director CNI, Informe Marty sobre cientos de vuelos CIA en Europa, rechazado), Grupo Parlamentario de Izquierda Verde-Izquierda Unida-Iniciativa per Catalunya Verds (07/03/2006, Director CNI, presentar documentos reunión gobierno-ETA en Zurich, 1999, rechazado), Grupo Parlamentario de Izquierda Verde-Izquierda Unida-Iniciativa per Catalunya Verds (13/03/2006, Director CNI, presentar documentos reunión gobierno-ETA en Zurich, 1999, rechazado), Coalición Canaria (22/03/2006, Director CNI, informe sobre muerte masiva de inmigrantes hacia Canarias, extinguido por desaparición o cese), PP (29/03/2006, Ministro Defensa, Informe CNI llegada de inmigrantes desde Mauritania), Grupo Parlamentario de Izquierda Unida-Iniciativa per Catalunya Verds (06/04/2006, Secretaria Estado de Defensa, conversaciones gobierno-ETA en Zurich, caducado), Grupo Parlamentario de Izquierda Unida-Iniciativa per Catalunya Verds (18/05/2006, Director CNI, explicar vuelos CIA en España tras informes Consejo y Parlamento Europeo y Amnistía Internacional, caducado), Grupo Parlamentario de Izquierda Unida-

Iniciativa per Catalunya Verds (07/06/2006, Director CNI, explicar Vuelos de la CIA, caducado), Gobierno (16/06/2006, Director CNI, explica presunto uso de aeropuertos españoles para traslado de detenidos en vuelos internacionales), Grupo Parlamentario de Izquierda Unida-Iniciativa per Catalunya Verds (01/02/2007, Director CNI, desclasificación documentos Audiencia Nacional sobre vuelos de la CIA, caducado), Grupo Parlamentario de Izquierda Unida-Iniciativa per Catalunya Verds (08/02/2007, Director CNI, vuelos de la CIA arrestos y traslados ilegales a centros de custodia y tortura, caducado), PP (15/06/2007, Director CNI, seguimiento de policías y CNI a empresarios españoles, caducado), PP (15/06/2007, Ministro Defensa, seguimiento de policías y CNI a empresarios españoles, caducado), PP (15/06/2007, Ministro Interior, seguimiento de policías y CNI a empresarios españoles, caducado), Gobierno (25/07/2007, Director CNI, explicar detención de un ex-agente del CNI), PP (25/07/2007, Director CNI, explicar detención del agente Roberto Flores Garcia, acusado de alta traición por revelar material secreto del Centro).

IX Legislatura (2008-2011) Iniciativas encontradas 22

PP (06/05/2008, Director CNI explicar caso rescate "Playa Bakio"), Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds (20/05/2008, Director Intel, explicar objetivos anuales del gobierno para el área de inteligencia), Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds (22/05/2008, director, vuelos de la CIA en España), PP (30/05/2008, Vicepresidenta explicar seguimiento del CNI al magistrado Roberto Garcia Calvo, rechazado), Gobierno (13/06/2008, Ministro Interior y Defensa, explicar el uso de gastos de ese año), Gobierno (16/10/2008, cumplimiento ley 11/2002), Comisión de control de gastos reservados (Director CNI, explicar seguimiento del CNI al magistrado Roberto Garcia Calvo), PP (19/11/2008, Director CNI, explicar demisión jefe división de inteligencia contraterrorista), PP (21/11/2008, Ministro Industria, supuesta injerencia rusa en Repsol, subsumido en otra iniciativa), Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds (02/12/2008, Vuelos de la CIA en aeropuertos españoles), PP (26/05/2009, Director CNI, explicar los más de 30 relevos en la directoria de contra-terrorismo en los últimos años), Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds (16/06/2009, situación interna e imagen CNI), Gobierno (19/06/2009 , gestión de CNI, uso de créditos presupuestarios), Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds (14/09/2009, situación interna y reorganización del Centro), Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds (14/09/2009, situación tropas españolas en Afganistán), PP (22/09/2009, Director CNI, explicar gestión del centro y cambios internos), Gobierno (28/09/2009, cumplimiento Ley 11/2002), Convergencia i Unio (18/11/2009, liberación del barco Alakrana, negociaciones con secuestradores), PP (19/11/2009, papel CNI en la liberación del barco Alakrana), Comisión de control de gastos reservados (17/12/2009, Ministros Interior Defensa, explicar el uso de créditos reservados), Grupo Parlamentario de Esquerra Republicana-Izquierda Unida-Iniciativa per Catalunya Verds (03/09/2010, Director CNI, explicar situación de tropas españolas en Afganistán), PNV (24/01/2011, Director CNI, explicar supuesta vigilancia sobre PNV y del Lehendakari Ibarretxe).

X Legislatura (2011-2016) Iniciativas encontradas 16 (en orden inversa)

Gobierno (11/12/2012, informar sobre uso y aplicación de fondos reservados); gobierno (caducado, 11/12/2012, comparecencia del director CNI por motivos de la ley11/2002); Convergencia i unió (18/02/2013, espionaje CNI a dirigentes políticos, sociales y empresariales), Izquierda Unida, ICV-EUia, CHA (28/02/2013, créditos inteligencia y caso Corinna), Izquierda Unida ICV-EUia, CHA (06/03/2013, CNI y hacker argentino Matias Malivacqua caso Nóos), Union Progreso y Democracia (19/03/2013, Caso Flayeh al Malayi, traductor detenido en Iraq, caducado), Convergencia y Unio (10/04/2013, Operación "Horizonte Después" epígrafe 10 millones "proyecto de tareas", convoca director CNI, caducado), Convergencia y Unio (10/04/2013, Operación "Horizonte Después" epígrafe 10 millones "proyecto de tareas", convoca Vice-presidente, caducado), Grupo Parlamentario de IU, ICV-EUiA, CHA: La Izquierda Plural (05/08/2013, relación CNI con Daniel Galván Viña, preso en Marruecos, indulto Rey, caducado), Grupo Parlamentario de IU, ICV-EUiA, CHA: La Izquierda Plural (23/10/2013, medidas de contra-inteligencia tomadas por España ante las revelaciones de Snowden, Vigilancia masiva NSA), Gobierno (30/10/2013, Director CNI llamado a informas sobre la Vigilancia masiva NSA), Grupo Parlamentario de IU, ICV-EUiA, CHA: La Izquierda Plural (05/11/2013, Caso Snowden, papel CNI es epsionage de organizaciones políticas en Euskal Herria y resto del Estado, caducado), PNV (03/02/2014, Director CNI convocado informar Directiva de Inteligencia 2014), Gobierno (24/06/2014, cumplimiento ley 11/2002), PNV (21/01/2015, Director CNI convocado informar Directiva de Inteligencia 2015).

XI Legislatura (2016-2016) Iniciativas encontradas 0 (2016-2016)

XII Legislatura (2016-2019), Iniciativas encontradas: 19

Autor: PP (03/01/2019, gastos de viaje Presidente), Grupo Mixto (13/12/2018, Ministerio de Interior y caso Barcenas), Grupo Mixto (01/08/2018 fondos operativos Guardia Civil), Gobierno (16/07/2018, Caso Villarejo), Podemos (caducado, 11/07/2018, Caso Corina, amenazas del director CNI), Podemos (caducado, 11/07/2018, caso Abdelabky es Sabdi), Socialistas (26/11/2017, Injerencia extranjera en Cataluña), Gobierno (09/06/2017, Directiva de Inteligencia 2017), Gobierno (09/06/2017, Uso de Fondos Reservados), Ciudadanos (19/05/2017, Director del Centro Criptologico, Wanacry y seguridad empresas, caducado), Ciudadanos (16/05/2017, Wanacry y seguridad estado, tramitado), Socialistas (12/05/2017, Wanacry de forma general), Unidos Podemos (22/03/2017, espionaje altas autoridades Estado, Director CNI), Unidos Podemos (22/03/2017, espionaje altas autoridades Estado, Vicepresidente), Esquerra Republicana (31/01/2017, Irregularidades uso de fondos para encubrir comportamiento de instituciones del Estado), PNV (31/01/2017, enfrentamiento CNI cuerpos policiales), PNV (31/01/2017, director CNI informar directiva de inteligencia 2017), Unidos-Podemos (04/11/2016, Fichero del CNI sobre Pablo Iglesias).

Annex II

Mixed Commission for the Control of Intelligence Activities (CCAI). Report of sessions per year (in Portuguese)

19/03/2014 | 1ª, Reunião
15:00
Instalação
4ª SESSÃO LEGISLATIVA ORDINÁRIA DA 54ª LEGISLATURA
Em 19 de março de 2014
Assunto / Finalidade:
Reunião de trabalho para dar posse ao Presidente da Comissão.

22/04/2014 | 2ª, Reunião
14:30
Reunião de Trabalho
Finalidade:
Definição conjunta do Cronograma de Trabalho.
Observação: A reunião será secreta com base no art. 22 da Resolução nº 2 de 2013-CN.

21/05/2014 | 3ª, Reunião
14:30
Reunião de Trabalho
Finalidade:
Definição conjunta do Cronograma de Trabalho.
Observação: A reunião será secreta com base no art. 22 da Resolução nº 2 de 2013-CN.
Conovocar General José Joselito, GSI, prestar esclarecimentos materia Joranl O Globo sobre alainça entre Movimento Sem Terra e Governo Venezuelano. (Autor Domingos SAvio, PSDB, REvoluçao Socialista). FIca aprovado o requerimento mas nao havendo quorum regimental, a pauta nao procede e fica prejudicada sua apreciaçao.

12/11/2014 | 4ª, Reunião
14:30
Reunião de Trabalho
FInalidade: Apreciação de Requerimentos.
Observação: a Reunião será secreta com base no art. 22 da Resolução nº 2, de 2013 - CN. Requerimento nº 15 de 2014 - CCAI, de
autoria do Deputado Domingos Sávio, é aprovado. Solicitada verificação de votação pelo Deputado Sibá Machado, Vice-Líder da Maioria na Câmara, representando o respectivo Líder, em virtude do anúncio "Aprovado o Requerimento".Não havendo quórum regimental, fica prejudicada a apreciação da matéria e dos demais Requerimentos constantes da Pauta da Reunião.

18/11/2014 | 5ª, Reunião
16:00
Reunião de Trabalho
NAO REALIZADA
Finalidad: Apreciação de Requerimentos.
Observação: a Reunião será secreta com base no art. 22 da Resolução nº 2, de 2013 - CN.

25/11/2014 | 5ª, Reunião
16:00
Reunião de Trabalho
CANCELADA
Finalidade:
Apreciação de Requerimentos.

09/04/2015 | 1ª, Reunião
14:30
Deliberativa
ADIADA
Finalidade:
Apreciação de Requerimentos.

28/04/2015 | 1ª, Reunião
14:30
Deliberativa
Finalidade:
Apreciação de requerimentos
Petiçao para realizar visitas pessoais às instalaçoes da ABIN, do Departamento de Inteligencia do Ministerio de Defesa, aos Centros de Inteligencias das Forças Armadas. e à Diretoria de Inteligencia Policial da Polícia Federal.
Motivo de fiscalizaçao e controle por parte da Comissao. (Autoria JÒ Moraes - PCdoB).
Petiçao Comparecimento do General José Elito, materia da Folha de Sao Paulo denuncia a tentativa de recrutamento de jovens ao Estado Islâmico. Autor Aloysio Nunes, PSDB.
Mesmo autor solicita esclarecimentos sobre possivel infiltraçao de agentes cubanos no Programa Mais Médicos.
Resultado: São aprovados os Requerimentos da Comissão de Atividades de Inteligência (RAI) de nº 2 a 6.

05/05/2015 | 2ª, Reunião
14:30
Audiência
Assunto / Finalidade:
Audiência com o Ministro-Chefe de Segurança Institucional da Presidência da República
Convidado:
Sr. José Elito Carvalho Siqueira
Ministro-Chefe do Gabinete de Segurança Institucional da Presidência da República. Inicio das comunicaçoes aberta em audiencia. Falas do GSI e ABIN em caráter secreto.
"Como falei inicialmente, isso é apenas um nivelamento, já que temos 12 Senadores e Deputados integrando a Comissão, começando os trabalhos após a instalação, mas gostaríamos de destacar, em cima desse conjunto que aqui foi mostrado, o aspecto da dinâmica do dia a dia, ou seja, grandes eventos para o Sistema têm que ser o dia a dia. Se praticarmos o grande evento diariamente, já que é um grande evento um país continental como este, com mais 700 cenários – é claro que pode haver dois mil, três mil, dependendo do foco –, se praticarmos só isso, só essa dinâmica imposta por este gigante Brasil, quando chegar um grande evento ocasional, como será o caso das Olimpíadas, como foi o caso da Copa do Mundo, apenas apertaremos o botão ou continuaremos o trabalho. Claro que será de uma forma mais ampliada, mas a rotina será absolutamente semelhante. Isso é fundamental. O trabalho do Sistema é muito mais importante no seu dia a dia, e é isto que exercitamos sempre." (José Elito em resposta a Jo Moraes)

07/07/2015 | 3ª, Reunião
14:30
Deliberativa
FINALIDADES
seja realizado, sob os auspícios da Comissão Mista de Controle das Atividades de Inteligência, o Seminário Internacional intitulado ATIVIDADE DE INTELIGÊNCIA NO ESTADO DEMOCRÁTICO, para tratar de tema essencial para o regime democrático e as atribuições do Poder Legislativo.
(Autora Jo Moraes)
1) Balanço da atuação da inteligência nos grandes eventos realizados no Brasil nos últimos anos, em especial os Jogos Mundiais Militares, a Copa das Confederações, a Jornada Mundial da Juventude e a Copa do Mundo de Futebol; 2) O papel da inteligência na segurança dos Jogos Olímpicos e Paraolímpicos de 2016, com os convidados que especifica. (Autora Jo Moraes) que seja requerido perante o ministro do Gabinete de Segurança Institucional, General José Elito, relatório sobre as atividades de inteligência e contrainteligência desenvolvidas pelo respectivo órgão ou entidade do SISBIN. (Autora Jo Moraes)
RESULTADOS:
requerimentos aprovados

14/07/2015 | 4ª, Reunião
14:30
Audiência Pública
Assunto / Finalidade:
Reforma da Legislação Brasileira de Inteligência.
Requerimento(s) de realização de audiência:
- RAI 5/2015, Deputada Jô Moraes
- RAI 10/2015, Deputada Jô Moraes
Participantes: Sr. Denilson Feitoza Pacheco
• Presidente da Associação Internacional para Estudos de Segurança e Inteligência Sr. Joanisval Brito Gonçalves
• Consultor Legislativo do Senado Federal especializado em Inteligência e Controle da Atividade de Inteligência
Sr. Edmar Furquim Cabral de Vasconcellos Junior
• Oficial de Inteligência
(representante de: Agência Brasileira de Inteligência (Abin))
RESULTADOS DELIBERAÇAO (excertos):
"Então, meus pontos de interesse aqui são uma política nacional de Inteligência. Eu me pergunto: como vai a CCAI fazer controle se não sabe para quê o sistema funciona. A Política Nacional de Inteligência é o objetivo. Nós existimos, estamos funcionando para isso. Então, quando se controla, controla-se comparado com algo. Desde 1988 não temos um plano nacional de Inteligência, o último foi lá, extinto em 1988. No Plano Nacional de Informações estava contida, anunciada a política nacional.
O Parlamento fez sua lição. Primeiro, o parlamento não foi tão bem, porque a primeira política nacional que entrou no Parlamento ficou aqui e está aqui até hoje, mas a segunda, a CCAI foi rápida, chegou em dezembro de 2009, em agosto de 2010 liberou, já mandou ao Governo Federal, que, aliás, é uma polícia nacional muito boa, muito bem atualizada, teve a participação de vários órgãos, inclusive o controle parlamentar. É uma política nacional plenamente atualizada. Eu me pergunto como todos os órgãos do Sibin podem estar atuando sem uma política nacional. O que todo mundo está fazendo? Essa é uma indagação. E como vão fazer o controle disso se não sabemos quais os objetivos?" (SR. Denilzon Feitoza Pacheco).

"Agora, a grande realidade é que se conhece muito pouco sobre a atividade de Inteligência. Qual é o grande objetivo de Inteligência? Temos que ter isso em mente antes de falar de legislação de Inteligência. O objetivo fundamental da Inteligência, senhoras e senhores, Deputada Jô Moraes, é assessorar um processo decisório, onde houver alguém tomando decisão, seja de um tenente que comande um pelotão de fronteira no extremo ocidental da Amazônia ao comandante do Exército; um delegado de uma regional ao secretário de segurança pública; um governador de Estado ao Presidente da República; um senhor de uma grande corporação. Todas essas pessoas que têm que decidir precisam de assessoramento adequado, com informações específicas que só a Inteligência pode fornecer. São informações produzidas por uma metodologia própria, que lidam com um dado negado e, de novo, que têm como fim assessorar esses tomadores de decisão." (Joanisval Brito)
"E a gente precisa de uma legislação adequada, por exemplo, no campo da interceptação telefônica. O Edmar já assinalou aqui. Nós precisamos de uma legislação que estabeleça mandatos claros, atividade de acompanhamento e competência para realizar, o Edmar chegou a citar inquérito, um processo administrativo. É ridículo o Estado brasileiro ter um serviço de inteligência que não possa fazer uma interceptação telefônica. Mas não é para buscar saber sobre a vida de A, B ou C. É porque quando nós tivemos um espião estrangeiro atuando aqui, foi preciso ter acesso às comunicações dessa pessoa; quando nós tivermos alguém que seja suspeito de ações terroristas, é inconcebível que a Inteligência não possa acessar as comunicações dessas pessoas." (Joanisval Brito)
"Precisamos da PNI, não dá mais, de 2009 para cá são quatro anos, cinco sem uma Política Nacional de Inteligência, que foi aprovada por esta Casa, precisamos revisar alguns aspectos da legislação de acesso à informação. A Lei de Acesso à Informação, Deputada, precisa ser revista para ser direcionada e o tratamento dado à informação de Inteligência tem que ser diferente." (Joanisval Brito)

11/08/2015 | 5ª, Reunião
14:30
Deliberativa
FINALIDADES E RESULTADOS
Seja convidado o MinistroChefe da Casa Civil da Presidência da República para comparecer a esta Comissão com
o objetivo de apresentar suas considerações sobre a demora na publicação da Política Nacional de Inteligência (PNI). (Autor Aloysiio Nunes)
Resultado: Retirado da Pauta
Discutir o balanço da atuação da inteligência nos grandes eventos realizados no Brasil nos últimos anos, em especial os Jogos Mundiais Militares, a Copa das Confederações, a Jornada Mundial da Juventude e a Copa do Mundo de Futebol; e o papel da inteligência na segurança dos Jogos Olímpicos e Paraolímpicos de 2016. Autora: Jo Moraes
Resultado: Aprovado

01/09/2015 | 6ª, Reunião
14:30
Reunião de Trabalho
Finalidade:
Discussão dos trabalhos propostos pela Comissão.
CANCELADA

06/10/2015 | 6ª, Reunião
14:30
1ª PARTE - Deliberativa, 2ª PARTE - Reunião de Trabalho
FINALIDADE

"seja convidado o MinistroChefe da Casa Civil da Presidência da República para comparecer a esta Comissão com
o objetivo de apresentar suas considerações sobre a demora na publicação da Política Nacional de Inteligência (PNI)." (senador Aloysio Nunes)
APROVADO
" a realização de Audiência Pública desta Comissão Mista para tratar da REFORMA DA LEGISLAÇÃO BRASILEIRA DE INTELIGÊNCIA, tendo como convidados Associação Nacional dos Oficiais de Inteligência – AOFI; e Associação dos Servidores da Agência Brasileira de Inteligência – ASBIN. Requer, por fim, que a presente audiência pública seja aberta." (deputada Jo Moraes)
APROVADO

13/10/2015 | 7ª, Reunião
14:30
1ª PARTE - Audiência Pública, 2ª PARTE - Deliberação sobre as Emendas da Comissão ao PLN nº 7/2015 (PLOA)
FINALIDADES
1) Balanço da atuação da inteligência nos grandes eventos realizados no Brasil nos últimos anos, em especial os Jogos Mundiais Militares, a Copa das Confederações, a Jornada Mundial da Juventude e a Copa do Mundo de Futebol; 2) O papel da inteligência na segurança dos Jogos Olímpicos e Paraolímpicos de
2016.
Requerimento(s) de realização de audiência:
- RAI 9/2015, Deputada Jô Moraes
- RAI 15/2015, Deputada Jô Moraes
- RAI 17/2015, Senador Aloysio Nunes Ferreira
Participantes: Eduardo Paes (Prefeito Rio de Janeiro), William Murad (Diretor Inteligencia da Secretaria Segurança para grandes eventos), Wilson Trezza (Diretor ABIN), Coronel Marcelo Rodrigues (Contra-inteligencia do Estado Maior)
RESULTADOS
Resultado: Foram apresentadas 27 emendas, 26 de apropriação e uma de texto. É aprovado Relatório, que conclui pela apresentação das Emendas nº 01 a 04-CCAI, correspondentes às emendas n°s 24, 25, 26 e 27 conforme o quadro de emendas, ao Projeto de Lei do Congresso Nacional nº 7, de 2015 (PLOA 2016) perante a Comissão Mista de Planos, Orçamentos Públicos e Fiscalização - CMO.
RECHO AUDIENCIA:
SR. HERÁCLITO FORTES (PSB - PI) – Dr. Trezza, desfaça uma curiosidade aqui. Vocês estão fazendo algum estudo, acompanhando de perto essa questão, que é gravíssima, que é a questão migratória?
O SR. WILSON ROBERTO TREZZA – Sim, estamos.
O SR. HERÁCLITO FORTES (PSB - PI) – Nós estamos um problema...
O SR. WILSON ROBERTO TREZZA – Estamos fazendo.
O SR. HERÁCLITO FORTES (PSB - PI) – Sobre a questão migratória, Presidente Jô, nós criamos uma comissão específica para ver isso. Eu vim de um encontro na Itália que reuniu todos os países da América e do Caribe. Nós estamos recebendo compulsoriamente migrantes que estão vindo de regiões muitas delas pacíficas e outras nem tanto. E trazem tecnologias de outros aprendizados.
Temos a questão do Haiti, que já convivemos a duras penas, mas esse é um tema que tomou conta do mundo. E está preocupando o mundo inteiro. Vai servir para a Olimpíada, mas vai servir para o Brasil no futuro. É muito grave essa questão migratória no mundo e o Brasil não está fora do contexto.
O SR. WILSON ROBERTO TREZZA – O senhor tem razão e nós trabalhamos com esse aspecto. O start foi dada pela migração irregular haitiana para o Brasil. Mas hoje temos

cerca de 16 nacionalidades que estão ingressando no Brasil também de maneira irregular. Irregular no sentido de não virem documentados, passam pela fronteira, pedem visto de refugiado e estão entrando no País. São mais de 16 nacionalidades. Mesmo que venham de locais do mundo onde a situação é pacífica isso continua sendo um problema. Mas nós estamos acompanhando e informando ao Governo. (p. 25-27)
[...] O SR. WILSON ROBERTO TREZZA – E só um último comentário, Presidente, em relação... O senhor mencionou sobre a Abin. Essa é a minha opinião, como Diretor da Abin, órgão central do Sistema Brasileiro de Inteligência, e já disse nesta Comissão e em outros lugares, e faço questão de frisar esse aspecto, que nós temos na Abin, como valores institucionais, sermos absolutamente apolíticos e apartidários. Então, acho que estando no ministério A, no ministério B, no ministério C, no nosso caso, internamente, não vamos mudar o nosso procedimento.
Eu não quero discutir questões das decisões que foram tomadas, onde colocar a Abin ou não, mas o senhor tenha certeza de que nós temos a competência para fazer o nosso trabalho. E a única coisa que diferencia a inteligência brasileira das melhores inteligências do mundo é: orçamento adequado, uma legislação que dê amparo à atividade de inteligência e acesso à tecnologia; e vamos cair de novo em orçamento, porque tecnologia é de uma celeridade muito grande, a obsolescência é rápida e custa caro.
Se nós temos um País com 204 milhões de habitantes, 7ª economia do mundo, com aspirações de ter um assento no Conselho Permanente de Segurança da ONU, nós precisamos reforçar a nossa estrutura de inteligência, defesa e segurança no País. E como eu costumo dizer, tudo começa pela inteligência. Se a inteligência trabalhar bem, segurança e defesa vão trabalhar menos e com melhores resultados.
A SRª PRESIDENTE (Jô Moraes. PCdoB - MG) – Obrigada, Dr. Trezza. Desculpe...
O SR. HERÁCLITO FORTES (PSB - PI) – Eu só quero dizer ao Dr. Trezza que quando levanto essa questão é porque quero que a Abin seja independente. Eu acho até que ela poderia ser ligada diretamente à Presidente da República.
A SRª PRESIDENTE (Jô Moraes. PCdoB - MG) – Nós vamos fazer essa...
O SR. HERÁCLITO FORTES (PSB - PI) – Porque a quem ela deve se reportar é à Presidente da República. A partir do momento que você coloca a Abin dependendo de um Ministro que toma conta dos secos e molhados, não vai evitar de, amanhã, até por ignorância de quem pede, alguém chegar ao Ministro e dizer: "Olha, diga lá ao Dr. Trezza para não ficar mais futricando a vida de fulano". E aí? Entendeu? Eu estou lhe dizendo apenas... Eu quero evitar esse constrangimento!
O SR. WILSON ROBERTO TREZZA – Eu entendo.
A SRª PRESIDENTE (Jô Moraes. PCdoB - MG) – Deputado Heráclito, nós vamos debater esse tema inclusive na próxima reunião. Esta Presidência concorda com V. Exª. Se tem de criar uma agência ligada diretamente à Presidência. Mas eu queria que a gente concluísse esta Mesa, que os Deputados e Senadores já precisam sair.
Nosso Coordenador, Willian Morato, com aquela proposta da Deputada Soraya, da informação e de uma nova reunião sigilosa.

15/10/2015 | 7ª, Reunião
14:30
1ª PARTE - Audiência Pública, 2ª PARTE - Deliberação sobre as Emendas da Comissão ao PLN nº 7/2015 (PLOA)
FINALIDADES
Continaçao da reuniao anterior
RESULTADOS
Diante do exposto, votamos no sentido de que esta Comissão Mista de Controle das Atividades de Inteligência – CCAI – delibere pela apresentação de 4 emendas de apropriação (itens 1 a 4) ao Projeto de Lei nº 7, de 2015-CN, destinadas às seguintes ações e unidades orçamentárias:

1. “14SY - Apoio à Realização de Grandes Eventos” (acréscimo) do Ministério da Defesa - Administração Direta de R$ 30.000.000,00;
2. “2866 - Ações de Caráter Sigiloso” (acréscimo) do Comando da Marinha, no valor de R$ 10.000.000,00;
3. “20XJ - Desenvolvimento Tecnológico do Exército” (acréscimo) do Comando do Exército, no valor de R$ 20.000.000,00.
4. “2684 - Ações de Inteligência” (acréscimo) da Agência Brasileira de Inteligência – Abin, no valor de R$ 60.000.000,00; e”
Relembramos à Comissão que as emendas devem fazer-se acompanhar da ata desta reunião, na qual se especificará a decisão aqui tomada. Também sugerimos que a Secretaria da Comissão adote as providências que se fizerem necessárias à formalização e à apresentação das emendas junto à Comissão Mista de Planos, Orçamentos Públicos e Fiscalização.

10/11/2015 | 8ª, Reunião
14:30
Audiência Pública
Assunto / Finalidade:
Discutir sobre Reforma da Legislação Brasileira de Inteligência
Requerimento(s) de realização de audiência:
- RAI 18/2015, Deputada Jô Moraes
Participantes: Carlos Terra Estrela (Presidente Associaçao dos Servidores de Inteligencia), Luciano Jorge (Vice-presidente Associaçao Oficiais de Inteligencia)
TRECHO PITORESCO:
Então, nós temos uma Política Nacional de Inteligência completamente defensiva e reativa. Não apontamos o que é importante para o Estado brasileiro. Isso tem que ficar bastante claro. Como poderíamos reescrever isso? Por exemplo, uma das diretrizes da Política Nacional de Inteligência deveria ser a segurança das comunicações. O que significa segurança das comunicações? Não é só proteger as nossas comunicações por meio de criptografias, base de dados brasileiras. Não! É mais que isso. Se os senhores não sabem, o Brasil tem um único satélite geoestacionário por qual passam todas as telecomunicações brasileiras. Esse satélite geoestacionário, que fica sobre o Brasil, não é brasileiro. Ele é mexicano; o dono dele é o Carlos Slim. Se alguém calcular errado, se alguém deixar cair café sobre a mesa de controle e desviar dois segundos o ângulo desse satélite geoestacionário, o Brasil perde a sua capacidade de se comunicar. Mandar mensagem pelo WhatsApp, ligar pelo celular, tudo isso acabaria. A internet, no Brasil, praticamente acabaria. Então, quando falamos de segurança das comunicações, é mais do que simplesmente defender contraespionagem e melhorar as capacidades de criptografia brasileiras.

31/05/2016 | 1ª, Reunião
15:00
Audiência
Assunto / Finalidade:
Audiência com o Ministro-Chefe de Segurança Institucional da Presidência da República.
Participante: General de Exército Sergio Westphalen Etchegoyen, Ministro-Chefe do Gabinete de Segurança Institucional da Presidência da
República
Resultado: Audiência realizada
Nao há notas sobre a reuniao, nem dados nem videos.

28/06/2016 | 2ª, Reunião
14:30

Emendas da Comissão ao PLN nº 2, de 2016 (PLDO).
Coordenador das Emendas: Deputado Pedro Vilela
REUNIAO CANCELADA

18/10/2016 | 2ª, Reunião
14:30
Emendas da Comissão ao PLN nº 18, de 2016 (PLOA).
Finalidade:
Deliberação sobre as Emendas da Comissão ao PLN nº 18, de 2016 (PLOA).
Coordenador das Emendas: Deputado Pedro Vilela
Resultado: A Comissão aprova a apresentação das seguintes 4 (quatro) emendas de apropriação à despesa ao PLN nº18 de 2016 (PLOA):
(1) Unidade Orçamentária Comando do Exército, Ação 147F – Implantação de Sistema de Defesa Cibernética para a Defesa Nacional, valor R$ 70.000.000,00; (2) Unidade Orçamentária Comando da Marinha, Ação 2866 – Ações de Caráter Sigiloso, valor R$ 1.000.000,00; (3) Unidade Orçamentária Agência Brasileira de Inteligência, Ação 2684 – Ações de Inteligência, valor R$ 10.000.000,00; e (4) Unidade Orçamentária Departamento de Polícia Federal, Ação 15F9 – Aprimoramento Institucional da Polícia Federal, valor R$ 80.000.000,00.

29/11/2016 | 3ª, Reunião
14:30
Audiência
Assunto / Finalidade:
Audiência
Participante:
General de Exército Sergio Westphalen Etchegoyen
• Ministro de Estado Chefe do Gabinete de Segurança Institucional
Resultado: Audiência realizada.
Nao se encontraram notas taquigráficas

03/04/2017 | 1ª, Reunião
17:00
Instalação
Assunto / Finalidade:
Posse da Presidente da Comissão, Deputada Bruna Furlan, e do Vice-Presidente, Senador Fernando Collor.
Resultado: Realizada a Reunião.

19/10/2017 | 2ª, Reunião
10:00
1ª PARTE - Deliberativa, 2ª PARTE - Deliberativa - Emendas ao PLOA 2018, 3ª PARTE - Audiência
FINALIDADES
Encaminha, para apreciação, os textos da proposta da Política Nacional de Defesa, da Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional.
Relatório: Pela aprovação nos termos do Projeto de Decreto Legislativo que o apresenta.
Resultado: Aprovado o relatório
/Deliberativa - Emendas ao PLOA 2018
Finalidade:
Deliberação sobre as emendas da Comissão ao PLN nº 20/2017 (PLOA 2018)
Anexos da Pauta
Quadro Descritivo - Emendas PLOA

Emendas CCAI - PLOA 201
"1. U.O. 52.121 – Comando do Exército, Programa 2058 – Defesa Nacional, Ação 147F – Implantação de Sistema de Defesa Cibernética para Defesa Nacional , valor R$ 70.000.000,00 (Propostas de emenda nºs 1 (Senador Jorge Viana), 5 (Deputado Luiz Ségio), 6 (Deputado Heráclito Fortes) e 8 (Deputado Benito Gama));
2. U.O. 52.131 – Comando da Marinha, Programa 2058 – Defesa Nacional, Ação 2866 – Ações de Caráter Sigiloso, valor R$ 3.600.000,00 (Propostas de emenda nºs 2 (Senador Jorge Viana), 3 (Deputada Bruna Furlan), 4 (Deputado Luiz Ségio) e 7 (Deputado Heráclito Fortes)); e
3. U.O. 20.118 – Agência Brasileira de Inteligência, Programa 2101 – Programa de Gestão e Manutenção da Presidência da República, Ação 2684 – Ações de Inteligência, valor R$ 40.000.000,00 (Proposta de emenda nº 9 (Deputada Bruna Furlan))."
Relatório
Resultado: Aprovadas as emendas apresentadas
/Realização de Audiência
Participante:
General de Exército Sergio Westphalen Etchegoyen, Ministro de Estado Chefe do Gabinete De Segurança Institucional da Presidência da República
Resultado: Audiência realizada (secreta)
EMENDAS REJEITADAS PELA COMISSAO DO PLOA

18/10/2018 | 1ª, Reunião
10:00
Deliberação de emendas a serem apresentadas ao PLOA 2019
Finalidade:
Deliberação de emendas a serem apresentadas ao PLOA 2019
Anexos do Resultado
Quadro das Emendas apresentadas
Relatório
Resultado: Aprovadas as seguintes emendas:
Emenda nº 1 – CCAI – Tipo: Apropriação/Acréscimo – Unidade Orçamentária 52.121 – Comando do Exército, Programa 2058 – Defesa Nacional, Ação 147F – Implantação de Sistema de Defesa Cibernética para Defesa Nacional, valor R$ 70.000.000,00;
Emenda nº 2 – CCAI – Tipo: Apropriação/Acréscimo – Unidade Orçamentária 52.131 – Comando da Marinha, Programa 2108 – Programa de Gestão e Manutenção do Ministério da Defesa, Ação 2866 – Ações de Caráter Sigiloso, valor R$ 5.000.000;
Emenda nº 3 – CCAI – Tipo: Apropriação/Acréscimo – Unidade Orçamentária 52.111 – Comando da Aeronáutica, Programa 2108 – Programa de Gestão e Manutenção do Ministério da Defesa, Ação 2866 – Ações de Caráter Sigiloso, valor R$ 20.000.000; e
Emenda nº 4 – CCAI – Tipo: Apropriação/Acréscimo – Unidade Orçamentária 20.118 – Agência Brasileira de Inteligência, Programa 2101 – Programa de Gestão e Manutenção da Presidência da República, Ação 2684 – Ações de Inteligência, valor R$ 80.000.000,00

Annex III

Media coverage of intelligence.
Number of articles published by Spanish newspapers and main topics addressed.

El País

TAG: CNI
2019 (until June): 5
2018: 35 (Villarejo case, Iman Ripollés connection with Barcelona attacks, Corinna case, and Pequeño Nicolás case)
2017: 18
2016: 13
2015: 21 (Nicolás case)
2014: 23 (cybersecurity, change of CNI Director)
2013: 53 (Ziani case, double agent)
2012: 9
2011: 11
2010: 32 (spy Flores stole information from the CNI)
2009: 76 (internal changes, international operations)
2008: 21
2007: 65 (Participation in Guantanamo, Afghanistan, CIA Flights, ETA)
2006: 45 (CIA flights)
2005: 43 (post-11-M attacks)
2004: 196 (11-M Madrid bombings and commissions of inquiry)
2003: 125 (war in Iraq, death of CNI agents)
2002: 21
2001: 10 (proposal to create a new CESID)

El Mundo

Tag: CNI
2019: 38 (Villarejo, Corina case)
2018: 99 (attacks in Barcelona, Catalan separatism)
2017: 107
2016: 100
2015: 102
2014: 147 (Nicolás case)
2013: 84
2012: 31
2011: 51
2010: 67
2009: 163 (international actions (Alakrana case), anti-terrorism)
2008: 46
2007: 70
2006: 74
2005: 50
2004: 128 (Madrid bombings, 11-M)
2003: 71
2002: 17
2001: 19

ABC.es

Tag: National Intelligence Center
2019: 19
2018: 63 (successful operations, such as the arrest of jihadists; CNI Director affirms that the intelligence avoids 2 attacks / day)
2017: 63
2016: 35
2015: 49
2014: 70
2013: 90
2012: 31
2011: 48
2010: 58
2009: 116 (Resignation of Alberto Saiz, Control Commissions, ETA detainees)
2008: 42
2007: 88 (Afghanistan War, Trashorra case, CIA flights repercussion)
2006: 73
2005: 67
2004: 176 (control of the CNI, Madrid terrorist attacks, 11-M)
2003: 141 (CNI agents killed in Iraq, Iraq war)
2002: 27
2001: 24 (the legal framework for the CNI is approved)

El Diario

Tag: CNI
2019: 22
2018: 108
2017: 98 (Iman Ripollés case, cyber attacks, Cloacas de Interior case)
2016: 89 (Villarejo case)
2015: 69 (defense commissions, Hacking team case)
2014: 66 (CNI budgets)
2013: 48 (Snowden revelations)
2012: 12
2011: 27
2010: 32
2009: 28
2008: 6
2007: 22
2006: 2
2005: 1
2004: 8

Público

Tag: CNI
2019: 18
2018: 59
2017: 37
2016: 25
2015: 29
2014: 9
2013: 13

2012: 1
2011: 1
2010: 15
2009: 37
2008: 5
2007: 2

Annex IV

Media coverage of intelligence.
Number of articles published by Brazilian newspapers and main topics addressed.

Folha de São Paulo
Tag: ABIN
2019: 22 until June (changes in ministries, appointment of university leaders, security in general)
2018: 40 (organized crime, regression in intelligence, data analytics and Facebook in Brazil, new Minister of Defense)
2017: 24 (fake news, alleged use of the ABIN to spy the Supreme Court after President Temer was linked with JBS prevarication, ABIN espionage of indigenous people and NGOs during Dilma Presidency)
2016: 66 (massive protests, Olympic Games and FIFA World Cup, alleged ISIS threats denied by the French Embassy)
2015: 22 (preparation for the games)
2014: 25 (secret spending on cards, Satiagraha repercussions)
2013: 102 (Case Romeu Tuma Jr, denunciation book: STF ministers tapped; spying diplomats; public security, ABIN infiltrated in social movements, growing protests)
2012: 55
2011: 30 (Government does not release secret documents from the 90s: nuclear program, terrorism, NGOs in the Amazon)
2010: 45 (WikiLeaks with documents about Brazil, hydroelectric dams in the Amazon)
2009: 204 (ABIN monitors trade unions and MST through a fake company, Senate Commission, ABIN director admitted this punctual action; Satiagraha repercussions; Inquiry Commission to clarify clandestine wiretaps)
2008: 522 (Satiagraha Operation, CPI of staples, removal of Paulo Lacerda, director of ABIN)
2007: 51 (SNI documents were destroyed, says ABIN)
2006: 31 (Organized Crime faction PCC expands, relations between ABIN and PF)
2005: 96 (archives of the dictatorship transfers to National Archives, scandal of the "mensalao", Financial Audit Federal Office, TCU, must audit Presidency, Casa Civil, and ABIN
2004: 65 (Army denies having files on Araguaia guerrilla from the 70s, ABIN expands its presence in third countries)
2003: 44 (Secret government spending, infiltration in social movements, organized crime)
2002: 63 (terrorism, organized crime)
2001: 47
2000: 98 (ABIN in BNDS investigations, enacted the first Congress Committees, members of the SNI vs. ABIN)
1999: - (in editorials) 32 (print and opinion) (ABIN creation and wiretapping scandal)

Globo
2019: 35 (O Globo) + 34 (G1) = 69 (until June)
2018: 34 (O Globo) + 55 (G1) = 89
2017: 46 (G1)
2016: 63 (G1)
2015: 15 (G1)
2014: 37 (G1)
2013: 56 (G1) protests and Olympic Games preparation
2012: 36 (G1)
2011: 47 (G1) call for new agents
2010: 46 (G1) call for new agents
2009: -

Estadao
Tag: ABIN
2001: 18
2002: 29 (mafias, diplomacy, parliamentary committees)
2003: 10
2004: 27 (official secrets)
2005: 2
2006: 35
2007: 71 (Satiagraha repercussion)
2008: 713 (Satiagraha)
2009: 323 (ABIN restructuring, ABIN monitors MST landworkers)
2010: 97
2011: 105
2012: 69
2013: 144
2014: 42
2015: 35
2016: 72
2017: 68 (WhatsApp shutdown)
2018: 85
2019 (June): 64 (Moroleaks, Vazajato)

Carta capital
tag: ABIN
2019: 16
2018: 2
2017: 7
2016: 1
2015: 1
2014: 3
2013: 1
2012: 10

Carta Maior
tag: ABIN
from 2003 to 2019: 22

Annex V

Academic coverage of accountability:
Time series and articles published by intelligence journals.

Brazil

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – Vol. 1, n. 1 (dez. 2005)- . – Brasília: Agência Brasileira de Inteligência, 2005

Accountability articles:

- O controle da atividade da inteligencia: consolidando a democracia. Joanisval Brito Gonçalves p. 33-45.

- Ética profissional na atividade de Inteligência: uma abordagem jusfilosófica Osiris Vargas Pellanda p.53-69.

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – Vol. 2, n. 2 (abr. 2006)- . – Brasília: Agência Brasileira de Inteligência, 2006

Accountability articles (null)

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – Vol. 2, n. 3 (set. 2006) – Brasília: Abin, 2006 edicion 3.

Accountability articles

- Consolidaçao da ordem democratica na inteligencia brasileira. Ayupe Mota. pp 45 - 52

- Meritocracia no serviço público. Costa de Moraes. p. 59-70.

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – Vol. 3, n. 4 (set. 2007) – Brasília: Abin, 2005 - edicion 4.

Accountability articles (null)

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 5 (out. 2009) – Brasília: Abin, 2006.

Accountability articles

- consideraciones sobre a relaçao entre a inteligencia e seus usuarios. p.7-20.

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 6 (abr. 2011) – Brasília: Abin, 2005

Accountability articles

- A inteligencia no estado democratico, soluçoes e impasses. pp.7-14

- Direito aplicado a atividade de inteligencia: consideraciones sobre a legalidade da atividades de inteligencia no Brasil- p. 27-41.

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 7 (jul. 2012) – Brasília: Abin, 2005

Accountability articles (null)

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 8 (set. 2013). Revisada e Corrigida – Brasília: Abin, 2005

Accountability articles

-Lei de acesso a informaçao e os reflexos sobre a produçao de inteligencia na Policia Federal, p.47-58.

-O uso de Data Mining para a inteligencia de estado. Um estudo de caso. p. 99-108.

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 9 (maio 2015) – Brasília: Abin, 2005

Accountability articles

- nova sistematica de proteçao à intimidade. p.65-80

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 10 (dez. 2015) – Brasília: Abin, 2005

Accountability articles (null)

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 11 (dez. 2016) – Brasília: Abin, 2005

Accountability articles:

- Accountability e o controle financeiro das atividades de inteligencia: uma revisao teórica pp. 9-30

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 12 (dez. 2017) – Brasília: Abin, 2005

Accountability articles:

– Quando o Segredo é a Regra: Atividade de Inteligência e Acesso à Informação no Brasil

– A Modernização da Inteligência Estratégica na Perspectiva da Segurança Humana.

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência. – n. 13 (dez. 2018) – Brasília: Abin, 2005

Accountability articles:

– A Agenda Legislativa da ABIN: Análise das Proposições sobre Atividade de Inteligência de Estado no Congresso Nacional de 1997 a 2017.

Annex VI

Academic coverage of accountability:
Time series and articles published by intelligence journals.

Spain

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 1
Pages: 160 Publication: 30/11/2006
Accountability articles (null).

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 2
Pages: 160 Publication: 21/09/2007
Accountability articles:
- Problemas actuales del derecho de los servicios de inteligencia
- Intereses académicos compartidos: Hacia una comunidad Iberoamericana de Inteligencia

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 3
Pages: 186 Publication: 19/12/2007
Accountability articles:
- La seguridad Europea ante el reto informativo: Conjugar secreto y transparencia.

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 4
Pages: 240 Publication: 30/06/2008
Accountability articles (null).

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 5
Pages: 176 Publication: 14/12/2008
Accountability articles:
- ¿Quién vigilará a los vigilantes? (Reinventando a Juvenal ante el foro de Roma, en Perú y Sudamérica).
- Sistema Judicial, Secreto Económico y Secreto de Estado.

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 6
Pages: 272 Publication: 26/06/2009
Accountability articles (null)

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 7
Pages: 246 Publication: 30/12/2009
Accountability articles (null)

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 8
Pages: 280, Publication: 19/06/2010
Accountability articles:
- El nuevo enfoque legal de la inteligencia competitiva
- La comunidad de inteligencia en Ucrania: creación, estructura y regulación

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 9
Pages: 128 Publication: 30/01/2011
6 artículos
- Espionage económico - un desafio oara la proteccion de la Constitucion alemana

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 10
Pages: 180 Publication: 29/06/2011
Accountability articles (null)

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 11
Pages: 248 Publication: 18/01/2012
Accountability articles:
-Democracia, política pública de inteligencia y desafíos actuales: tendencias en países de Latinoamérica

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 12
Pages: 342 Publication: 20/12/2012
Accountability articles:
- La legislación italiana en materia de inteligencia
- Normas que regulan el régimen económico en el CNI
- El secreto de Estado en el Proceso Penal: entre la denegación de auxilio y el delito de revelación
- Marco teórico del control parlamentario de la seguridad nacional

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 13
Pages: 328 Publication: 31/05/2013
10 artículos

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 14
Pages: 190 Publication: 23/12/2013
Accountability articles (null)

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 15
Pages: 212 Publication: 29/06/2014
Accountability articles:
- Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo.

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 16
Pages: 176 Publication: 30/12/2014
Accountability articles:
- Informes de control de los Comités de Inteligencia parlamentarios como una fuente para la investigación

INTELIGENCIA Y SEGURIDAD: REVISTA DE ANÁLISIS Y PROSPECTIVA. Nº 17
Pages: 180 Publication: 14/03/2016
Accountability articles (null)

The International Journal of Intelligence, Security, and Public Affairs

Volume 18, 2016
Issue 1
-null
Issue 2
-Ethical implications of the Snowden revelations
Issue 3
-null

Volume 19, 2017
Issue 1
-null
Issue 2
-null
Issue 3
-Lessons through reform: Australia´s security intelligence

Volume 20, 2018
Issue 1
-The intelligence service in Costa Rica: Between the new and the old paradigm
Issue 2
-null
Issue 3
-Why are State secrets protected from disclosure? The discourse of Secret Keepers
Intelligence Control and Oversight in Poland since 1989

Volume 21, 2019
Issue 1
-Spy watching: intelligence accountability in the United States

Jaseff Raziel Yauri-Miranda worked as a researcher and lecturer in the Department of Political Science and Administration at the University of the Basque Country (UPV-EHU). He graduated in History and Political Science at the Federal University of Minas Gerais (UFMG-Brazil) and University of Santiago de Compostela (USC-Spain). His research fields included security policies, criminal law, intelligence, and surveillance studies. He received the Jean Pinatel Prize of Criminology in 2016. He published articles in many countries and participated in institutions such as the Harvard University, MA, USA; the International Association of Political Science, Capri, Italy; the Center for Strategic Studies on Intelligence, Belo Horizonte, Brazil; the International Group on Governance, (In)security and Intelligence, Babes-Bolyai, Romania; the Panteion University of Social and Political Sciences, Athens, Greece; and the Surveillance Studies Centre, Kingston, Canada.

This research was funded by the Basque Government FPI program.