

**GRADO: DOBLE GRADO EN ADMINISTRACIÓN Y
DIRECCIÓN DE EMPRESAS Y DERECHO**

2023/2024 Año Académico

TFG: DERECHO

**PROTECCIÓN DE DATOS PERSONALES EN
LA UE ANTE EL MARKETING DIGITAL
IMPULSADO MEDIANTE IA: ANÁLISIS
JURÍDICO-CONSTITUCIONAL**

AUTORA: MAIDER BAIGORRI ABERASTURI

DIRECTORA: LEIRE ESCAJEDO SAN EPIFANO

Departamento Derecho Público y Ciencias Histórico-Jurídicas y del Pensamiento Político

Bilbao, a 21 de junio de 2024.



ÍNDICE DE CONTENIDOS

1. CONTEXTO DEL TRABAJO, OBJETIVOS Y METODOLOGÍA	7
2. CONSTITUCIONALISMO DIGITAL Y SU POSIBLE REFLEJO EN LA PREOCUPACIÓN POR LA PROTECCIÓN DE DATOS EN EL CONTEXTO DEL MARKETING DIGITAL IMPULSADO MEDIANTE IA (<i>AI-POWERED DIGITAL MARKETING</i>)	10
2.1. Las nociones de IA a los efectos de su regulación jurídica.....	10
2.2. El marketing digital impulsado por la IA (<i>AI-Powered digital marketing</i>), con especial referencia al uso de <i>Chatbots</i> (o asistentes virtuales).....	15
3. LA EVOLUCIÓN DEL ESTATUTO JURÍDICO DE LA PROTECCIÓN DE DATOS PERSONALES EN LA UE, POR CUANTO RESPECTA AL <i>AI-POWERED DIGITAL MARKETING</i>.....	18
3.1. El derecho fundamental a la protección de datos respecto a la privacidad y la intimidad	19
3.2. Los principales instrumentos normativos de la Unión Europea referentes al <i>AI-Powered digital marketing</i>	22
3.2.1. El Reglamento General de Protección de datos personales (RGPD), con especial atención a la irradiación de los principios de su art. 5	23
3.2.2. El Paquete de Servicios Digitales (Reglamento de Mercados Digitales (RMD) y Servicios Digitales (RSD)	25
3.2.3. El reglamento de Inteligencia Artificial (RIA)	27
3.3. Algunas notas para tener en cuenta sobre el Paquete RDM-RSD y RIA, por cuanto afecta al marketing digital.....	30
4. CASO DE USO: LONUX, comercio textil online, incorpora a su página la aplicación virtual SIRA de proveedor NIVOL.....	33
4.1. Descripción del caso de uso	34
4.2. De la compra y puesta en el mercado de la UE de la aplicación SIRA (de proveedor estadounidense), para su uso por LONUX.....	37
4.2.1. La cuestión de la territorialidad de la aplicación SIRA a los efectos de la aplicación de RGPD y el RIA.....	37
4.2.2. La clasificación de “SIRA” en las modalidades de riesgo del RIA y sus implicaciones para la protección de datos	40
4.3. La captación de los datos de los usuarios en la interacción con el <i>Chatbot</i> de SIRA: datos personales y reconocimiento biométrico de emociones.....	41
4.4. El tratamiento automatizado de datos personales que realiza LIXUS a través de SIRA para poder ofrecer publicidad personalizada a los usuarios.	44

4.5. Impacto que tiene en la protección de datos el hecho de que SIRA sea un “Servicio Digital” que proporciona y mantiene NIVOL respecto a múltiples usuarios	46
4.6. Mecanismos que los usuarios finales de SIRA en el comercio online de LONUX tienen para proteger su derecho fundamental a la protección de datos	47
5. CONCLUSIONES.....	48
6. RECONOCIMIENTOS	51
7. BIBLIOGRAFÍA Y REFERENCIAS DOCUMENTALES.....	52
7.1 Bibliografía.....	52
7.2 Documentos Institucionales	56
7.3 Seminarios de expertos/ponencias	57
7.4 Normativa.....	57
7.5 Jurisprudencia.....	58

ÍNDICE DE IMÁGENES

Imagen 1: Funcionamiento Sistema IA.....	12
Imagen 2: Subtipos de IA.....	13
Imagen 3: Fases estrategia de marketing.....	17
Imagen 4: Jerarquía de riesgos.....	30
Imagen 5: Inversión en IA.....	31
Imagen 6: Patentes IA.....	31
Imagen 7: Esquema 1 Caso de Uso.....	35
Imagen 8: Esquema 2 Caso de Uso.....	36

ABREVIATURAS Y ACRÓNIMOS

AEPD	Agencia Española de Protección de Datos
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CE	Constitución Española de 1978
CEDH	Convenio Europeo para la protección de Derechos Humanos y de las Libertades Fundamentales (1950)
EEMM	Estados Miembros
EE. UU.	Estados Unidos
IA	Inteligencia Artificial
LOPDPGDD	Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales
OCDE	Organización para la Cooperación y el Desarrollo Económico
RGPD	Reglamento (UE) 2016/ 679 General de Protección de Datos
RIA	Reglamento (UE) 2024/ XXX de Inteligencia Artificial*
RMD	Reglamento (UE) 2022/ 1925 de Mercados Digitales
RSD	Reglamento (UE) 2022/ 2065 de Servicios Digitales
STC	Sentencia del Tribunal Constitucional
STS	Sentencia Tribunal Supremo
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TUE	Tratado de la Unión Europea
UE	Unión Europea

* NOTA: Esta es la forma de cita oficial del R.I.A., dado que no recibirá número hasta que se publique formalmente en el DOUE.

Resumen

La Brújula Digital Europea, presentada en 2021, reconoce que la pandemia de la COVID-19 que transformó el papel y la percepción de la digitalización en las economías y sociedades europeas y aceleró su implantación. Tiempo atrás, y con el objetivo garantizar para 2030 una soberanía digital acorde con su visión y sus valores, la Unión Europea había asumido ya el reto de dotarse de un marco de gobernanza compartido con los Estados Miembros, pivotado por una serie de reglamentos estratégicos. A ese conjunto de reglamentos estratégicos se ha incorporado recientemente el Reglamento de Inteligencia Artificial, del que se ha dicho viene a completar el nuevo constitucionalismo digital europeo. Inspirado en una tradición que nació en tiempos analógicos, este constitucionalismo aspira, entre otras cosas, a reforzar las dimensiones objetiva y subjetiva de los derechos fundamentales en el espacio digital.

El presente TFG, procede a testar la solidez de ese marco de garantías en su aplicación a la protección de datos personales en el marketing digital impulsado mediante inteligencia artificial (*AI Powered Digital Marketing*). Al efecto, se presentan las garantías a la protección de datos incorporadas a los instrumentos normativos ya aprobados (en especial, aunque no en exclusiva, en el RGPD, el RSD y el RIA), tales garantías se contextualizan en el marco de la Estrategia Digital Europea y, sobre esa base, se procede a su análisis jurídico-constitucional en una perspectiva teórico-práctica, con el apoyo de un caso de uso diseñado *ad hoc*.

Palabras clave: *inteligencia artificial, marketing digital, soberanía digital europea, derechos y libertades fundamentales, constitucionalismo digital, Reglamento General de Protección de Datos, Reglamento de Servicios Digitales y Reglamento de Inteligencia Artificial.*

Abstract

The European Digital Compass, presented in 2021, recognises that the COVID-19 pandemic did not originate, but rather transformed the role and perception of digitalisation in European economies and societies and accelerated its deployment. Some time ago, and with the aim of ensuring digital sovereignty by 2030, in line with its vision and values, the European Union had already taken up the challenge of providing itself with a governance framework shared with the Member States, pivoted by a series of strategic regulations. This set of strategic regulations has recently been complemented by

the Artificial Intelligence Act, which has been said to complete the new European digital constitutionalism. Inspired by a tradition born in analogue times, this constitutionalism aims, among other things, to enhance the objective and subjective dimensions of fundamental rights in the digital space.

This End of Degree Thesis tests the robustness of this framework of guarantees in its application to the protection of personal data in AI-powered digital marketing. To do so, the guarantees incorporated into the regulatory instruments already approved (especially, but not exclusively, the GDPR, the DSA and the AIA) are introduced, contextualised within the framework of the European Digital Strategy and their legal-constitutional analysis is carried out from a theoretical-practical perspective, with the support of a use case designed *ad hoc*.

Key words: *artificial intelligence, digital marketing, European digital sovereignty, fundamental rights and freedoms, digital constitutionalism, General Data Protection Regulation, Digital Services Act and AI Act.*

1. CONTEXTO DEL TRABAJO, OBJETIVOS Y METODOLOGÍA

En 2018 la cantidad de datos en todo el mundo ascendió a 33 zettabytes, con una previsión de que en 2035 la cifra fuera de 2.142 zettabytes¹. La irrupción de la IA en lo cotidiano promete aumentar exponencialmente ese intercambio masivo de datos. Hace más de una década que la UE, consciente de este nuevo contexto económico y social, y de la relevancia que en el presente y a futuro tienen la economía de datos y las innovaciones en inteligencia artificial, viene trabajando con intensidad sobre su estrategia digital. Destacan, entre los documentos políticos más tempranos, la Agenda Digital Para Europa, publicada en 2010, y la Estrategia para el Mercado Único Digital de 2015. A los mismos, les han seguido el Libro Blanco sobre la IA, la Estrategia Europea de Datos (2020), y la Brújula Digital (2021) junto con un índice - el “*Digital Economy and Society Index (DESI)*”- que mide la evolución de los Estados Miembros y la UE en competitividad digital, en áreas como la conectividad, el nivel de digitalización de las empresas y administraciones o la capacitación de las personas, entre otros. Desde el punto de vista normativo, asimismo, ha sido necesario reformular instrumentos jurídicos de relevancia, como la Directiva 95/45/CE de protección de datos personales (a la que sustituyó el R. (UE) 2016/ 679, RGPD), y formular textos jurídicos relativos al mercado de datos, los servicios digitales o la inteligencia artificial, entre otros.

Ursula von der Leyen, en su Discurso sobre el Estado de la Unión de septiembre de 2020² como presidenta de la Comisión, resumió todos estos esfuerzos en la siguiente idea: la UE busca garantizar su soberanía digital; al efecto necesita, de una parte, unas infraestructuras tecnológicas resilientes, seguras y fiables y, de otra, y, mecanismos que garanticen el respeto de los valores de la Unión. El objetivo es asentar un ecosistema en que se equilibren la excelencia y la confianza.

Son muchas las perspectivas jurídicas desde las que cabe analizar el Espacio Digital Europeo, su marco de gobernanza y su entramado regulador. En este trabajo, se ha optado por una perspectiva de análisis jurídico-constitucional que atiende a las garantías del derecho a la protección de datos en su aplicación al *AI-Powered Digital Marketing* o Marketing impulsado mediante IA. La mayor vulnerabilidad para la protección de datos

¹ Moreno, G./Statista Daily Data. (2019). *Infografía: A la espera de un Big Bang de datos*.

² Discurso Estado de la Unión 2020.

se produce, en concreto, cuando las empresas que comercian en línea emplean herramientas de IA en su interacción con las personas (clientes o no) que se acercan a sus páginas de comercio en línea.

Por su reciente aprobación y su trascendencia, entre las normas aprobadas por la UE destaca el RIA. De él se ha dicho que es una pieza clave del nuevo constitucionalismo digital europeo, destinado a reforzar los derechos fundamentales en el espacio digital³. Citando a dos importantes constitucionalistas, Cotino Hueso y Balaguer Callejón, las Constituciones “*se forjaron en un mundo analógico*”⁴ y son necesarios nuevos paradigmas que “*constitucionalicen el algoritmo y digitalicen la constitución*”⁵. La UE avanza en ese proceso, pero no hemos de olvidar las importantes concesiones que, al mismo tiempo, realiza respecto a los mercados y la innovación.

El análisis jurídico-constitucional y teórico-práctico de las garantías que los datos personales reciben respecto al marketing digital impulsado por la IA es **un tema que se ha escogido para este TFG por un doble motivo**. En primer lugar, porque se trata de un tema de actualidad que plantea importantes y urgentes retos a la disciplina del Derecho constitucional. La UE ha aprobado o revisado una serie de Reglamentos -como el RGPD, el Paquete de Servicios Digitales formado por el RMD y el RSD o el RIA⁶ - que, más allá de sus contenidos respecto a elementos esenciales del mercado o de las tecnologías disruptivas, resultan estratégicos para reforzar las dimensiones objetiva y subjetiva de relevantes derechos fundamentales⁷ como es caso, aunque no en exclusiva, del derecho a la protección de datos personales⁸. En segundo lugar, porque este trabajo ha permitido plasmar uno de los puntos de inflexión común que tienen tanto la carrera de ADE como de la de Derecho, al mismo tiempo que he tenido la posibilidad de estar vinculada durante

³ De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal Of Constitutional Law*, 19(1), 41-70.

⁴ Cotino Hueso, L. (2022). Nuevo paradigma en las garantías de los derechos fundamentales. En L. Cotino (dir) *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*. Aranzadi, p.68

⁵ Balaguer Callejón, F. (2022), *La constitución del algoritmo. El difícil encaje de la constitución analógica en un mundo digital*, Fundación Manuel Giménez Abad, pp.31-33.

⁶ Se ha utilizado como fuente para este trabajo el segundo texto de RIA que el Parlamento Europeo, tras corregir algunos errores, publicó en marzo de 2024.

⁷ Tajadura Tejada, J. (2021). *Los Derechos fundamentales y sus garantías*, 2ª edición, Tirant lo Blanch, p.42-43.

⁸ Presno Linera, M. A. (2022), *Derechos fundamentales e Inteligencia Artificial*, Marcial Pons, p.37.

6 meses al proyecto de investigación sobre IA y derechos fundamentales *AI-Biosurv* a través de una beca IKASIKER.

Determinar si en la UE el derecho fundamental de protección de datos personales está lo suficientemente salvaguardado respecto al marketing digital impulsado por IA ha sido el **objetivo** de la investigación. El análisis, se plantea además desde la perspectiva de los principios básicos de la protección de datos asentados en el Reglamento General de Protección de Datos.

El trabajo, en cuanto a su **estructura**, comienza con la exposición y explicación del marco normativo del marketing digital impulsado por la IA en el seno de la UE, y, a continuación, en perspectiva jurídico-constitucional, se analiza desde un punto de vista teórico y práctico la salvaguarda que la normativa europea ofrece al derecho fundamental a la protección de datos personales en dicho ámbito. Como herramienta de apoyo, en el abordaje práctico se ha diseñado un caso de uso *ad hoc*. Concluye el trabajo con un apartado final en el que se reflexiona sobre el potencial de las garantías vigentes y los desarrollos que aún están pendientes.

Por cuanto se refiere a la **metodología** empleada deben destacarse dos importantes elementos. De una parte, y, en primer lugar, este trabajo ha requerido el análisis de numerosas fuentes bibliográficas y documentales, seleccionadas tras un exhaustivo proceso de búsqueda. A la falta de publicaciones específicas que, a la fecha de elaboración del trabajo, analizasen marketing digital en perspectiva constitucional se ha añadido como principal dificultad la abundancia, imposible de abarcar, de publicaciones que de forma general abordan diferentes dimensiones jurídicas del uso de la IA. Entre las fuentes seleccionadas destacan monografías individuales y colectivas de reciente publicación pertenecientes al fondo bibliográfico del grupo de investigación en el que he participado, artículos de revistas indexadas y documentos oficiales, además de textos normativos, resoluciones de la AEPD y sentencias del TC y el TJUE. Para testar los hallazgos de la investigación documental respecto a la situación práctica, se ha diseñado ad hoc un caso prospectivo, proyectando sobre él el nivel de garantías vigentes.

2. CONSTITUCIONALISMO DIGITAL Y SU POSIBLE REFLEJO EN LA PREOCUPACIÓN POR LA PROTECCIÓN DE DATOS EN EL CONTEXTO DEL MARKETING DIGITAL IMPULSADO MEDIANTE IA (AI-POWERED DIGITAL MARKETING)

El marketing, que como es sabido es mucho anterior a la existencia de la propia IA, se ve impactado por esta última en dos importantes frentes: de una parte, la *tormenta* de explotación e intercambio de datos⁹ que se asocian con el uso intensivo de Big Data y la IA; de otra, una serie de nuevas vulnerabilidades para la seguridad y la protección de la privacidad y la protección datos¹⁰, en especial cuando las personas usuarias interactúan directamente con la IA.

Hasta la fecha no se han publicado normas específicas que den solución a esos impactos en la UE, aunque ello resulta comprensible si tenemos en cuenta que son muy pocos los países que cuentan siquiera con normas relativas a la IA en general. Según la OCDE, en el año 2019 muy pocos países habían desarrollado una estrategia nacional de IA¹¹. Por ver el lado positivo, las pocas estrategias existentes coinciden en una serie de rasgos objetivos y valores comunes, como el deseo de un crecimiento inclusivo, la justicia o los enfoques centrados en la persona. En contraste, una importante dificultad de la construcción de los marcos de gobernanza de la IA ha sido precisar qué debe entenderse por IA y cómo impacta esta, en concreto, en los derechos y libertades de las personas. Veamos en este contexto cuáles han sido las decisiones adoptadas por la UE.

2.1. Las nociones de IA a los efectos de su regulación jurídica

Se ha dicho de la IA que es una fuerza disruptiva “*que puede revolucionar industrias enteras y provocar cambios significativos*” en las prácticas comerciales¹². Igualmente, su actual crecimiento es consecuencia principalmente de: (i) el aumento de la capacidad de

⁹ Cotino Hueso, L. (2022), *op. cit.*, p 68.

¹⁰ Comisión Europea (2020, 19 de febrero). *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado en la excelencia y la confianza*. COM (2020) 65 final.

¹¹ OECD (2023), *The state of implementation of the OECD AI Principles four years on*, OECD Artificial Intelligence Papers, No. 3, OECD Publishing, Paris, p.11.

¹² Kumar, V., Ashraf, A. R., & Nadeem, W. (2024). AI-powered marketing: What, where, and how? *International Journal Of Information Management*, 102783.

almacenamiento, y (ii) de la rapidez de procesamiento de los datos almacenados¹³. Más allá de esas descripciones genéricas, el caso es que delimitar un concepto de IA relevante a efectos jurídicos no ha sido una tarea sencilla, porque se trata de un término muy discutido, incluso, en sus dimensiones técnicas.

El término técnico IA no es nuevo. Su primera definición se atribuye a John McCarthy, quien en una conferencia en Dartmouth College la definió en 1965 "*la ciencia y la ingeniería de hacer máquinas inteligentes, especialmente programas de computadora inteligentes*"¹⁴. La obsolescencia de esta definición, expuesta a los avances tecnológicos, y las importantes discrepancias entre los expertos explican que más de 70 años después sigamos, sin embargo, sin un concepto universalmente aceptado de IA. Por ese motivo, la literatura científica presenta las definiciones técnicas de IA distinguiendo diferentes niveles de inclusividad.

Podemos entender la IA como aquellos modelos computacionales que permiten emular una inteligencia similar a la humana (en capacidades como las de planificar y/o prever las consecuencias de las acciones)¹⁵ o, dicho de otra manera, como "*la habilidad de un ordenador digital o un robot controlado por un ordenador de realizar acciones o tareas comúnmente asociadas a seres inteligentes*"¹⁶. Esa definición obedece al hecho de que los sistemas de IA perciben e infieren mediante diferentes sensores y mecanismos de captación información de los entornos, y disponen de módulos que, empleando algoritmos y otros modelos matemáticos, son capaces de almacenar e interpretar esa información y de procesarla a los efectos de adoptar¹⁷ (véase la imagen 1).

¹³ Herrera de las Heras, R. (2022). *Aspectos legales de la inteligencia artificial: personalidad jurídica de los robots, protección de datos y responsabilidad civil*. Dykinson. S.L. p. 20.

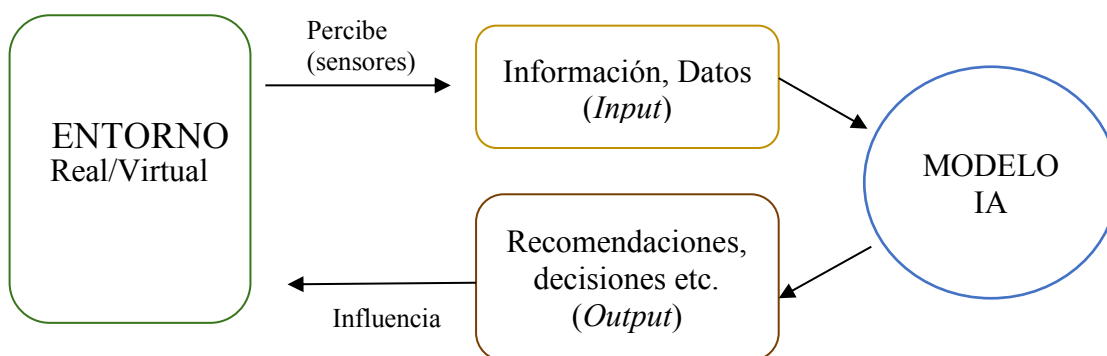
¹⁴ Gobierno de España. (2023). *Qué es la inteligencia artificial*.

¹⁵ Meseguer, P. y López de Mántaras, R. (2017). *Inteligencia artificial*. España: Los Libros de La Catarata. p. 7-8.

¹⁶ Traducción propia a partir de: Girasa, R. (2021). *Artificial Intelligence as a Disruptive Technology: Economic Transformation and Government Regulation*. Palgrave Macmillan. p. 8.

¹⁷ Comisión Europea, (2019a). *Una definición de la Inteligencia Artificial: Principales capacidades y disciplinas científicas*, Oficina de Publicaciones. p. 1.

Imagen 1: Funcionamiento Sistema IA



Fuente: elaboración propia a partir de Memorándum OCDE¹⁸; p.7

El nivel al que los sistemas de IA son capaces de emular la inteligencia humana varía, pero de forma importante, de ahí que se distingan, primero, dos grandes categorías de IA (la débil y la fuerte), y una serie de subcategorías o subgrupos.

- i. **IA Débil o específica:** “entendida como la ciencia e ingeniería que permite diseñar y programar ordenadores de forma que realicen tareas que requieren inteligencia”¹⁹. Se trata por lo tanto de la realización de una única tarea (limitada y específica) como puede ser jugar al ajedrez contra un humano o hacer una predicción de ventas²⁰.
- **IA Fuerte o general:** “entendida como la ciencia e ingeniería que permite replicar la inteligencia humana mediante máquinas”²¹. Es decir, aquella IA que es capaz de realizar la mayoría de las tareas que pueden realizar los seres humanos²².

¹⁸ OECD (2024). *Explanatory memorandum on the updated OECD definition of an AI system*, OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris. p. 4-6.

¹⁹ Meseguer, P. y López de Mántaras, R., (2017), *Op. cit.*, p.8

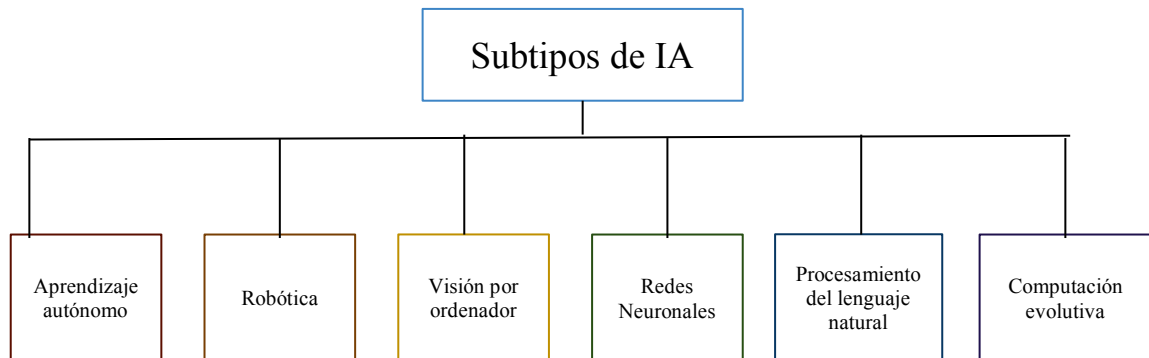
²⁰ Girasa, R., (2021), *Op. cit.*, p. 10.

²¹ Meseguer, P. y López de Mántaras, R. (2017), *Op. cit.*, p.8

²² Comisión Europea (2019a). *Op. cit.*, p.5

Por cuanto se refiere a los subgrupos, estos han sido organizados atendiendo a las alternativas que en la actualidad existen para poder “*aproximarse a una solución IA*”²³ (Ver Imagen 2).

Imagen 2: Subtipos de IA.



Fuente: elaboración propia a partir de Girasa, R. (2021); p.13.

Por cuanto se refiere al marketing digital, la subcategoría con mayor relevancia desde la perspectiva jurídica, será la de **aprendizaje autónomo** o “*machine learning*”. Este subtipo agrupa el tipo de sistemas de IA que, sin necesidad de ser programados, captan masivamente información y todo tipo de datos -incluyendo el reconocimiento de emociones- y, a partir de éstos, mejoran sus habilidades de actuación²⁴ y de toma de decisiones²⁵. En el contexto de este trabajo de investigación, y por cuanto se refiere a la protección de datos de las personas, esa tendencia a la captación masiva tendrá mucha relevancia.

Como es comprensible, esa falta de consenso sobre el concepto científico-técnico de IA ha tenido impacto en la elaboración de estrategias políticas y normas jurídicas sobre la IA. En cualquier caso, las discusiones en diferentes instituciones y foros de gobernanza no han perseguido definir la IA y precisar cuál debía ser el ámbito de aplicación de un marco regulador para la misma. Es importante señalar, además, que las normas jurídicas relativas a la IA, entre ellas el RIA -primera norma de estas características aplicada a nivel mundial- tienen una vocación de *lex specialis* en el conjunto de normas jurídicas que protegen la información y la captación y uso de todo tipo de datos. Entre esas normas

²³ AEPD. (2020, febrero). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción.* p. 5.

²⁴ Girasa, R. (2021), *Op. cit.*, p. 13.

²⁵ Comisión Europea (2020, 19 de febrero). *Libro Blanco ... Op. cit.*, p. 20.

destaca, por su relevancia respecto a los derechos y libertades fundamentales, el RGPD, pero existen también normas que protegen la información industrial o la competencia leal.

Las definiciones sobre IA que se han extendido en los marcos reguladores son definiciones que buscan ser lo suficientemente flexibles y amplias como para poder dejar margen a desarrollos futuros²⁶. La OCDE se refiere a este tipo de definiciones como definiciones inclusivas, que pretenden abarcar tanto lo más simple como lo más complejo, sin perjuicio de que, en algunos usos más específicos del término, en especial en la normativa, pueda procederse a una mayor delimitación de los conceptos relevantes²⁷.

Se busca ofrecer seguridad jurídica²⁸ a un entorno, el de la IA, inmerso en un proceso de desarrollo acelerado²⁹. La primera definición formal ofrecida en la UE es de 2018, en una Comunicación de la Comisión. En ella se describen “*los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos*”³⁰. En la misma línea, después de algunos intentos previos, la OCDE³¹ describirá la expresión sistema de IA como relativa a “*un sistema basado en máquinas que, para unos objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA varían en sus niveles de autonomía y adaptabilidad tras su despliegue*”³². Esta definición es la que finalmente ha sido incorporada al Reglamento de Inteligencia Artificial de la UE (art 3.1 RIA), donde se engloban tanto sistemas de *software* como de *hardware*³³.

²⁶ Comisión Europea (2020, 19 de febrero). *Libro Blanco ... Op. cit.*, p.12

²⁷ OECD (2024). *Op. cit.* p. 4-6.

²⁸ Filibi I. (2024, 24 de enero). *La estrategia digital europea y el proceso de elaboración del reglamento europeo de inteligencia artificial*. Seminario Iberoamericano de Expertos Hacia un marco regulador de la IA: Retos en perspectiva comparada, UPV/EHU. Bilbao, España.

²⁹ Comisión Europea (2020, 19 de febrero). *Libro Blanco ... Op. cit.*, p.20.

³⁰ Comunicación *Inteligencia Artificial para Europa*, Bruselas 25.4.2018 COM (2018) 237 final, p.1.

³¹ Cabe destacar la labor realizada desde la organización internacional en aras de buscar una definición que alcanzase el consenso entre diferentes culturas y economías. Fernández Hernández, C. (2024) *La OCDE explica el contenido de su definición actualizada de los sistemas de Inteligencia Artificial*, Diario La Ley de 6 de marzo de 2024.

³² Fernández Hernández, C. (2024). *Op. cit.*

³³ Rincón, M. A. (2024). Aproximación a la propuesta legislativa europea sobre inteligencia artificial. *Quaderns IEE: Revista de l'Institut d'Estudis Europeus*, 3(1), 110-124. p. 113.

2.2. El marketing digital impulsado por la IA (*AI-Powered digital marketing*), con especial referencia al uso de *Chatbots* (o asistentes virtuales)

El marketing, al igual que la sociedad ha ido evolucionado, y a pesar de que la forma en la que se conecta con los consumidores ha cambiado, su objetivo último sigue siendo la venta de determinados bienes y servicios. Se discuten el origen y la autoría de este término, aunque la mayor parte de la literatura dice que el término surge en los EE. UU. en la primera década del siglo XX³⁴ y fue Clark quien ofreció, en 1925, la primera definición formal, “*como el conjunto de esfuerzos que efectúan la transferencia de la propiedad de bienes y se ocupan de su distribución física*”³⁵. En la actualidad, y a consecuencia de los cambios económico, sociales y tecnológicos, este término abarca mucho más que un simple intercambio comercial. De hecho, la última de las definiciones dada por la *American Marketing Association* (AMA) en 2013 define esta disciplina como “*la actividad, conjunto de instituciones y procesos para crear, comunicar, entregar e intercambiar ofertas que tienen valor para los consumidores, clientes, socios y la sociedad en general*”³⁶. En una comparación entre la definición de Clark y la de la AMA, cabe destacar que las funciones del marketing han crecido más allá del ámbito puramente organizacional, en el sentido de que ya no solo generan , un valor no solo a las partes intervinientes, sino que a toda la sociedad en su conjunto³⁷.

En cuanto a sus herramientas, las posibilidades del marketing crecieron exponencialmente gracias a invenciones tan relevantes la imprenta o, siglos después, la publicidad en la radio o la televisión³⁸. De igual modo, la llegada de las nuevas tecnologías de la información y la comunicación (TIC) generará nuevas vías de comunicación con potenciales consumidores y usuarios, dando inicio al denominado *marketing digital*. Bajo este último término se entienden comprendidas “*todas las estrategias de mercado que realizamos en la web para que un usuario de nuestro sitio*

³⁴ García, J. S. (2014). Marketing hasta la última definición de la AMA (American Marketing Association). *Revista de la Asociación Española de Investigación de la Comunicación*, 1(2), 124-132. p. 125

³⁵ *Ibidem*. p. 126.

³⁶ *Ibidem*. p. 120.

³⁷ *Ídem*.

³⁸ Beard, F. K. (2017). The Ancient History of Advertising: Insights and Implications for Practitioners. *Journal Of Advertising Research*, 57(3), 239-244.

*concrete su visita tomando una acción que nosotros hemos planeado de antemano*³⁹”. La potencialidad para alcanzar públicos cada vez más creando perfiles de potenciales interesados, serán los cambios más destacables del marketing digital⁴⁰. Ejemplos tales como: los anuncios o *banners* en sitios webs, el marketing por correo electrónico (*email marketing*) o por redes sociales y los *newsletter* con ofertas personalizadas son solo algunas de todas las aplicaciones que puede llegar a tener el marketing digital⁴¹.

La llegada de la IA supone un nuevo hito respecto al marketing digital, siendo las principales novedades: (a) el cambio exponencial en la capacidad de obtención, procesamiento y almacenamiento de grandes cantidades de datos (tanto históricos como obtenidos en tiempo real); y (b) su potencial para elaborar perfiles de usuarios y ofrecer en tiempo real propuestas personalizadas de valor a los usuarios⁴². En relación con las capacidades relativas a los datos, en protección de datos tendrá relevancia que la información obtenida en tiempo real se combinará con información previamente almacenada y obtenida de fuentes muy diversas (como redes sociales, datos de navegación o datos obtenidos de asistentes virtuales de las personas en sus hogares, electrodomésticos o vehículos), o preferencias y tendencias en la adquisición de productos y servicios. Algunos de esos datos, aunque no todos, serán datos de carácter personal (art.4.1. RGPD), quedando abarcadas también bajo el RGPD algunas fórmulas de elaboración de perfiles (art.4.4 RGPD)⁴³.

La IA puede afectar a todas y cada una de las fases que comprende una estrategia de marketing digital: análisis del mercado, planificación, ejecución y evaluación (vid. imagen 3, infra).

³⁹ Selman, H. (2017). *Marketing digital*. Ibukku. p. 6.

⁴⁰ *Ibidem*. p.6.

⁴¹ *Ibidem*. p. 8-9.

⁴² Kingsnorth, S. (2019). *Digital Marketing Strategy: An Integrated Approach to Online Marketing*. Kogan. p.21.

⁴³ Se entiende por elaboración de perfiles toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos a [...] sus preferencias personales o intereses, o su ubicación (art. 4.14 RGPD).

Imagen 3: Fases estrategia de marketing.



Fuente: Elaboración propia, a partir de Loreto y Sanz, 2005.

En primer lugar, y por cuanto se refiere a la fase de **análisis** de mercado, la IA impacta en la capacidad para recoger datos, analizarlos y entender el comportamiento o detectar las emociones de los consumidores es esencial (tanto sus necesidades como sus gustos). En segundo lugar, en relación con la fase de **creación y planificación** de la estrategia, la IA facilita la segmentación del mercado, el posicionamiento de la marca y el “*target*” al que se quiere dirigir, al ser capaz de reconocer patrones y estándares del mercado. En tercer lugar, la IA también ofrece interesantes ventajas a la hora de **ejecutar** la estrategia de marketing, en especial en términos de personalización de los bienes y servicios, y en la creación de experiencias más gratificantes y personalizadas para los consumidores y usuarios.⁴⁴ Finalmente, en la última de las etapas, la IA puede contribuir en lo que la **evaluación** de los resultados se refiere, contando la misma además con sistemas de aprendizaje autónomo o “*machine learning*” que llevan incorporado la capacidad de mejora continuada.

Las formas en las que pueden ser introducidas tales mejoras son múltiples, como puede verse en algunos ejemplos ya implementados. Partiendo de la publicidad y de los anuncios en web, con aplicaciones tales como *GoogleAdWords* la IA es capaz de personalizar los mismos al poder analizar el comportamiento de los consumidores⁴⁵. Aplicaciones como *Receptiviti*, por su parte, facilitan la fidelización de los clientes actuales, mediante un análisis de “*los mensajes de texto y voz de las personas para revelar su psicología, personalidad, emociones y toma de decisiones*”⁴⁶, que, entre otras cosas, permite conocer de primera mano y en tiempo real las actitudes ante diferentes

⁴⁴ Huang, M. H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. *Journal of the Academy of Marketing Science*, 49, 30-50. p. 31-38

⁴⁵ Girasa, R., (2021), *Op. cit.*, p. 8.

⁴⁶ Medina-Chicaiza, R. P., y Martínez-Ortega, A. G. (2020). Tecnologías en la inteligencia artificial para el Marketing: una revisión de la literatura. *Pro Sciences: Revista De Producción, Ciencias e Investigación*, 4 (30), 36-47, p. 43.

ofertas. Estos análisis, además, pueden contribuir en el diseño de las diferentes páginas web ahorrando tiempo y coste económico⁴⁷ o a la creación de “micromomentos de interacción” personalizada⁴⁸. En este último sentido destacan especialmente los *bots* de charla (o Chatbots)⁴⁹. Estos sistemas simulan mantener una conversación con una persona, ya sea de forma textual o, en los casos más avanzados, de forma hablada (como sucede en el uso de *Amazon Alexa, Siri o Google Nest*).

3. LA EVOLUCIÓN DEL ESTATUTO JURÍDICO DE LA PROTECCIÓN DE DATOS PERSONALES EN LA UE, POR CUANTO RESPECTA AL AI-POWERED DIGITAL MARKETING

Dado que el crecimiento de la IA y sus perspectivas para la industria del marketing son inmensas⁵⁰, cabe preguntarse cuál es el nivel de garantías de que el derecho fundamental de protección de datos personales dispone en la UE. La IA no solo está invadiendo la esfera personal de los consumidores con el uso de sus datos, sino que los mismo también se están empleando para monitorear⁵¹ sus sentimientos afectado así también a la libertad de toma de decisiones de los propios usuarios. En menos de media década, la UE ha hecho un importante esfuerzo para ofrecer un marco de seguridad jurídica consistente tanto para los potenciales operadores e inversores, como para los ciudadanos.

Entre los hitos mas recientes está el Reglamento de Inteligencia Artificial, sin olvidar que, por su parte, el Consejo de Europa (CoE) aprobó en mayo de 2024 -pendiente de ratificación- un Convenio *Marco sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho* (CMIA). En su “Explanatory Report” insite el CoE en que la recolección de datos personales es actualmente ubicua y no sólo consiste en el manejo de datos previamente recolectados, sino que, además, permite inferir datos nuevos a partir de aquellos. Dado que los datos son una base muy relevante en numerosos modelos de negocio, a falta de una adecuada revisión de las garantías preexistentes el

⁴⁷ Girasa, R., (2021) *Op. cit.*, p. 8.

⁴⁸ Alet, J. (2024, 4 junio). La inteligencia artificial aplicada de forma ‘eficaz’ al marketing, *Revistas Harvard Deusto*.

⁴⁹ Medina-Chicaiza, R. P., y Martínez-Ortega, A. G., (2020) *Op. cit.*, p. 43.

⁵⁰ Kumar, V., Ashraf, A. R., & Nadeem, W. (2024), *Op. cit.*

⁵¹ Cuervo Sánchez, C. A. (2021). Efectos de la inteligencia artificial en las estrategias de marketing: Revisión de literatura. *Revista Internacional de Investigación en Comunicación ADResearch ESIC*, 24(24), 26-41. p. 38.

CoE prevé un aumento significativo de los riesgos para la privacidad de las personas⁵². Establece, en coherencia, que las partes firmantes deben adoptar o mantener las medidas necesarias para garantizar y proteger la privacidad y la intimidad de los datos personales a la largo del ciclo de vida de los sistemas IA (art. 11 del CMIA). Procede pues revisar, en concreto respecto al marketing digital impulsado mediante IA, cual es el nivel de garantías de que la UE dispone en la actualidad.

3.1. El derecho fundamental a la protección de datos respecto a la privacidad y la intimidad

Según Presno Linera, el mayor impacto de uso de los sistemas de IA se prevé respecto a derechos fundamentales que garantizan la dimensión privada las personas⁵³. Se advierte, además, de que la incidencia del tratamiento masivo de datos en los derechos de las personas no sólo tiene impactos individuales, sino una importante repercusión en la colectividad, generando, entre otras cosas, asimetrías de poder y una vigilancia con efectos intimidatorios. A este último respecto, autores como Hoffman-Riem consideran que, hasta la fecha, ha sido la dimensión subjetiva la que ha predominado en la defensa del derecho a la protección de datos, pero que ha llegado el tiempo de desarrollar con más detalle la dimensión objetiva de la protección de este derecho fundamental -pensando en especial, en el impacto de las captaciones masivas de datos respecto a la colectividad-⁵⁴. En este orden de cosas, aunque no se refiere expresamente a la dimensión colectiva del derecho a la protección de datos, cabe traer a colación una reciente sentencia del Tribunal Constitucional Español, STC 27/2020, en la que indica que es inadmisibles que “sólo por el hecho” de comunicarse a través de entornos digitales o de beneficiarse de internet, las personas no deben ver sacrificados sus derechos fundamentales⁵⁵.

La CDFUE dedica especial atención a la dimensión privada de las personas en sus artículos 7 y 8, mientras que textos que le precedieron, como el CEDH de 1950 o la Constitución Española de 1978, lo hacen respectivamente en sus arts. 8 y 18. Conviene, no obstante, recordar que intimidad, privacidad y protección de datos son términos que

⁵² Consejo de Europa (2024). *Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, p. 18

⁵³ Presno Linera, M. A. (2022), *op. cit.*, p.37

⁵⁴ Hoffmann-Riem, W. (2019). *Big data: desafíos también para el Derecho*. Civitas, p.102.

⁵⁵ FJ 3º STC 27/2020.

se refieren a la dimensión privada de las personas, aunque no sinónimos entre sí. El término privacidad es el que abarca una esfera más amplia, englobando todo aquello que se tiene derecho a no intromisión por ser parte de la vida privada de una persona, y intimidad, por su parte hace referencia según la RAE a la “*zona espiritual íntima reservada de una persona*”, de modo que, según la STS 1495/ 2024 de 3 de marzo, lo que concierne a la intimidad concierne a privacidad, pero no todo lo que atañe a la vida privada forma necesariamente parte de lo íntimo, al ser este último un concepto de dimensión más deducida. . Por cuanto se refiere a la relación entre la protección o reserva de datos y el derecho a la intimidad la misma sentencia reconoce que ambos conceptos “*tienen evidentes caracteres comunes*”, pero que *no todo acceso a datos protegidos constituye por sí misma una violación del derecho a la intimidad*”.

Por cuanto se refiere a la normativa de la UE y su desarrollo jurisprudencial, tal y como se ha expuesto, el artículo 8 de la CDFUE (2000) reconoce que “*toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan*”, recogido como un derecho diferente al de la privacidad. Dada su relevancia, el art 16 TFUE establece las obligaciones y competencias de desarrollo legislativo que corresponden al Parlamento Europeo y al Consejo en esta materia⁵⁶. No fue hasta el año 2008 cuando el TJUE se refirió expresamente al derecho fundamental a la protección de datos, en la STJUE de 29 de enero de 2008, C-275/06-⁵⁷. En su jurisprudencia más reciente, el TJUE combina sistemáticamente dos derechos, el derecho a la privacidad y del derecho a la protección de datos, si bien su respectivo alcance. Se trata de dos derechos distintos y que el derecho a la protección de datos otorga a las personas más derechos y sobre más tipos de datos que el derecho a la privacidad.⁵⁸

Respecto a la Constitución Española, doctrina y jurisprudencia coinciden en reconocer que se trata de un derecho no reconocido expresamente, aunque abarcado en el art. 18 CE⁵⁹. Es más, se podría decir que es un derecho que tiene su origen en el de intimidad,

⁵⁶ Herrera De las Heras, R. (2022). *Op. cit.*, p.53.

⁵⁷ Concellón, P. (2018). El concepto de dato personal en la Unión Europea: una pieza clave en su protección. *Revista General de Derecho Europeo / General Journal Of European Law*, 46, p. 8

⁵⁸ Lynskey O. (2014). Deconstructing Data Protection: The ‘Added-Value’ of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly*. 63(3):569-597.

⁵⁹ Fernández, J. M. (2003). El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario. *DS: Derecho y Salud*, 11(1), 37-46. p. 37.

pero se trata de una evolución del mismo principalmente por la irrupción de las TIC⁶⁰. En la doctrina jurisprudencial de TC destaca la pionera STC 292/2000 del 30 de noviembre. En la misma, (i) se definió por un lado el derecho a la protección de datos como derecho independiente e individualizado, desvinculado del derecho a la intimidad del artículo 18 CE⁶¹, así como (ii) se aportó luz respecto al concepto de datos personales y a los elementos configuran este derecho -entre ellos las facultades que asisten al titular del mismo-, siendo además esta la línea jurisprudencial que se sigue empleando en la actualidad. El derecho a la protección de datos garantiza, en esencial, un poder de control de las personas sobre sus datos (FJ. 6º de la STC 292/ 2000), que, en su desarrollo normativo, se ha concretado en derechos como los que siguen: derecho de acceso (art. 15 RGPD), derecho de rectificación (art.16 RGPD), derecho de oposición (art. 21 RGPD), derecho de supresión o del olvido (art 17 RGPD), derecho a la limitación del tratamiento (art. 18 RGPD), derecho a la portabilidad (art. 20 RGPD), derecho de información (arts. 13 y 14) y derecho a no ser objeto de decisiones individualizadas (art. 22RGPD)⁶².

Como consecuencia de la irrupción de los Big Data y del tratamiento masivo de datos que permitirá la IA, adquirirá especial notoriedad **la cuestión de qué datos pueden entenderse como personales y cuáles no**. La jurisprudencia del TJUE ha ido evolucionando al ritmo que las nuevas tecnologías también lo han hecho, viéndose ampliado cada vez más el término de dato personal. Dicha evolución, se ve reflejada en la definición aportada por el RGPD (art. 4), inspirado en la doctrina del TJUE. Se define como dato personal *“toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”*.

Por lo tanto, observamos como se trata de un término con un gran alcance ya que se engloba cualquier información que nos permita identificar a una persona o, incluso, re-

⁶⁰ Herrera De las Heras, R. (2022). *Op. cit.*, p.54.

⁶¹ Fernández, J. M. (2003) *Op. cit.*, p. 37.

⁶² AEPD (2024, 8 de marzo). *Derechos y deberes*. <https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos/derecho-de-acceso>

identificarla cuando, con pocas garantías, se haya procedido a una *pseudoanonimización*. Ejemplo de ello son: “*un nombre, un apellido, una matricule de un vehículo, un teléfono, un número de pasaporte, una dirección IP, un perfil vinculado a una persona en cualquiera de los ámbitos antes citados cualquier otro identificador único, incluidos datos o conjuntos de datos que actúen como seudoidentificadores, y los vinculados a los mismos*”⁶³. Sin embargo, es cierto que no todos los datos gozan de la misma protección⁶⁴, aplicando mayores garantías la normativa vigente a datos tales como el origen étnico o racial, opiniones políticas o religiosos, datos biométricos o las orientaciones sexuales entre otros (art. 9 RGPD).

Dada la relevancia que el reconocimiento biométrico de emociones tiene en el marketing digital impulsado mediante IA conviene, no obstante, hacer algunas precisiones sobre los datos biométricos. Son datos biométricos aquellos datos que, aplicando un procedimiento técnico, captan y digitalizan información anatómico-física (p.ej., procedente de una huella o de un rostro), información fisiológica (velocidad del latido o temperatura corporal) o información comportamental (p.ej. las emociones). El procedimiento técnico es relevante, dado que no se capta un rostro en formato de foto o imagen, sino que se procede, por ejemplo, a calcular su geometría facial, localizando y registrando las distancias que median, por ejemplo, entre las pupilas de los ojos, las distancias entre barbilla, punta de la nariz y partes prominentes de los pómulos, así como la estructura del conjunto del rostro⁶⁵. Conforme al RGPD sólo son datos biométricos aquellos que permitan captar la identidad única de una persona (art. 4.14 RGPD); ello plantea una importante duda sobre el estatuto de datos biométricos no identificantes, como pueden ser los que se usan en el reconocimiento de emociones y captan, por ejemplo, la ira, la alegría o la tristeza en el rostro de una persona.

3.2. Los principales instrumentos normativos de la Unión Europea referentes al *AI-Powered digital marketing*

⁶³ AEPD (2023, septiembre). *Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo*. p.5.

⁶⁴ Herrera De las Heras, R. (2022). *Op. cit.*, p.56.

⁶⁵ L. Escajedo San Epifanio, Tecnologías biométricas, identidad y derechos fundamentales, Aranzadi, 2017, 84-85.

Hasta la aprobación del RIA y otros textos que serán objeto de análisis, el RGPD, a pesar de sus limitaciones respecto a los datos masivos no personales, era el mayor y prácticamente *único refugio* ante la fuerte tormenta de intercambio masivo de datos que experimentamos en la actualidad⁶⁶. Como se verá, al menos por cuanto respecta al marketing digital impulsado mediante IA, el RGPD mantendrá esa posición estratégica.

Aunque no son específicos respecto al *AI-powered digital marketing*, son 3 los textos jurídicos más relevantes en lo que se refiere a la protección de datos en este ámbito: el RGPD, el Paquete que conforman el Reglamento de Mercados Digitales y el de Servicios Digitales, y el Reglamento de Inteligencia Artificial. Los tres se presentan a continuación, y su nivel de garantías será testado en el apartado 4, en su aplicación al caso de uso diseñado *ad hoc*.

3.2.1. El Reglamento General de Protección de datos personales (RGPD), con especial atención a la irradiación de los principios de su art. 5

El RGPD derogó y sustituyó en 2016 la Directiva 95/46/CE⁶⁷ y ha sido recientemente actualizado por el Reglamento (UE) 2023/2854, sobre normas armonizadas para un acceso justo a los datos. El ámbito de aplicación de este Reglamento, que desarrolla en España Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales⁶⁸, es el tratamiento de los datos personales, lo que significa que engloba cualquier tipo de operación (automatizadas o no) realizada sobre datos personales o conjunto de estos. Se entiende por operación entre otros a: “*la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*”⁶⁹. Por cuanto se refiere a la IA, es relevante que el RGPD aplica respecto aquellos datos personales que corresponden a personas físicas identificadas o identificables y, hasta cierto punto, a las personas *reidentificadas*⁷⁰.

⁶⁶ Ni Loideain, N. (2018). A Port in the Data-Sharing Storm: The GDPR and the Internet of Things. *King's College London Law School Research Paper*, nº 2018

⁶⁷ Fernández Villazón L. A. (2016). El nuevo Reglamento Europeo de Protección de Datos. *FORO. Revista de Ciencias Jurídicas y Sociales, Nueva Época*, 19(1), 395-411.)

⁶⁸ Preámbulo LOPDPGDD.

⁶⁹ AEPD (2023, septiembre). *Orientaciones para...*, *Op. cit.*, p.5.

⁷⁰ Cotino Hueso, L. (2022). *Nuevo paradigma...*, *Op. cit.* 89.

El RGPD es también el texto jurídico de referencia en el tratamiento de la elaboración de perfiles⁷¹, actividad muy relevante en el marketing digital y a la que se refieren también el Paquete RDM-RSD y el RIA⁷². Y, por cuanto se refiere a las garantías institucionales en materia de protección de datos, ha de destacarse que el RGPD creó un órgano de control para el cumplimiento de la normativa con competencia para dictar directrices, recomendaciones y establecer las buenas prácticas⁷³: el Comité Europeo de Protección de datos. El mismo, está compuesto tanto por todas las autoridades de control nacionales, como es la Agencia Española de Protección de Datos en España, las cuales habrán de cooperar conjuntamente (art 60 RGPD)⁷⁴, así como por el Supervisor Europeo de Protección de Datos.

En lo que se refiere a las proyecciones del RGPD respecto al Paquete RDM-RSD y el RIA, ha de destacarse el relevante rol que desempeñan los principios generales que, según el art.5 RGPD, deben respetarse en cualquier tratamiento de datos personales. Se trata en concreto de los principios de: (a) Licitud, lealtad y transparencia; (b) Limitación de la finalidad; (c) Minimización de datos; (d) Exactitud; (e) Limitación del plazo de conservación; (f) Integridad y confidencialidad; (g) Responsabilidad activa.

La Directiva 95/46, sustituida por el RGPD, recogía en su articulado los principios de legitimidad, finalidad, necesidad y proporcionalidad en sentido estricto, que se consideran comprendidos y ampliados en el nuevo listado al que se ha hecho referencia. Ha generado cierta preocupación que el término licitud venga a sustituir, en el RGPD, la expresión legitimidad, por cuanto que en la Teoría del Derecho la expresión legitimidad se asienta sobre la existencia de un mandato legal, mientras que licitud parece apelar simplemente a la conformidad con el Derecho y, por tanto, con independencia del sujeto que trate los datos. Aunque la interpretación literal de ambos términos pueda no ser la misma, la AEPD ha avanzado que ambos se han de entender en el mismo sentido, ya que el RGPD no rebaja la protección ofrecida por la Directiva, sino que la amplía y *“recoge las mismas bases jurídicas que contenía la Directiva”*⁷⁵.

⁷¹ Fernández Villazón L. A. (2016). *Op. cit.*, p.400.

⁷² Así, en los considerandos del RIA.

⁷³ Unión Europea. (s. f.). *Comité Europeo de Protección de Datos (CEPD)*.

⁷⁴ Fernández Villazón L. A. (2016). *Op. cit.*, p.406.

⁷⁵ AEPD (s. f.-a). *¿cuáles son las bases de legitimación para el tratamiento de datos?*

Debe destacarse también que los conceptos de necesidad y proporcionalidad en el tratamiento de los datos han quedado abarcados en el RGPD por una nueva idea, la de minimización de los datos. La idea de minimización hace referencia a que el tratamiento de los datos, dentro de la finalidad que lo legitima, debe ser en términos de cantidad y calidad lo menos intrusivo posible. Ello implica: “*mínima cantidad de datos personales, mínima extensión del tratamiento, mínimo plazo de conservación y mínima accesibilidad a datos personales*”⁷⁶. Sin embargo, es cierto que, en el contexto actual, la minimización de datos será complicada de alcanzar con el uso masivo de datos que caracteriza a las IA⁷⁷.

3.2.2. El Paquete de Servicios Digitales (Reglamento de Mercados Digitales (RMD) y Servicios Digitales (RSD))

El Paquete que conforman la Ley de Servicios Digitales y la Ley de Mercados Digitales es una pieza clave en la consecución de la soberanía digital europea, por cuanto se traducen en una mayor supervisión pública de las grandes plataformas digitales y contribuyen a dotar de seguridad el espacio digital, reforzando la protección de los derechos fundamentales de los usuarios y estableciendo unas condiciones de competencia equitativas para las empresas⁷⁸.

En concreto, el **RSD** (2022), establece las condiciones para que en el mercado interior surjan y se desarrollen servicios digitales, entendidos los mismos como plataformas/intermediarios que operan en línea, como es el caso de los proveedores de *de servicios de internet, servicios en la nube, mensajería, mercados o redes sociales*⁷⁹. Por cuanto se refiere al tema que nos ocupa, destaca que el RSD combina la atención a las reglas de la competencia con la atención a la seguridad física y psíquica y a los derechos de los usuarios⁸⁰. Por su parte, el **RMD** centra la atención en los llamados “*guardianes*

⁷⁶ AEPD (2023). *Protección de datos por defecto*.

⁷⁷ Herrera De las Heras, R. (2022). *Op. cit.*, p.59.

⁷⁸ Cordero Álvarez, C. I. (2024) El régimen de responsabilidad de las plataformas online en la DSA. En Castelló Pastor (dir.), *Análisis del reglamento (UE) de Servicios Digitales y su interrelación con otras normas de la UE*, Aranzadi, 71-72.

⁷⁹ Comisión Europea. (2024, 3 febrero). *Preguntas y respuestas sobre la Ley de Servicios Digitales*.

⁸⁰ Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, (2024). *El Reglamento de Servicios Digitales (Digital Services Act - DSA) explicado*. p. 2

de acceso” o grandes proveedores de servicios de plataforma, que actúan como intermediarios clave entre las empresas y los consumidores, a los que desde marzo de 2024 se les exige cumplir con una serie de obligaciones.

En el objeto de análisis del presente trabajo, el marketing digital, el RSD contempla “*cualquier tipo de publicidad, desde la comercialización digital hasta la publicidad basada en temas y los anuncios políticos*”⁸¹, y, además, complementa las normas vigentes, como el RGPD, ya que establece entre otras normas sobre el consentimiento de los usuarios o su derecho a oponerse a la comercialización digital⁸². Además, en la línea con lo que establece el artículo 22 del RGPD anteriormente mencionado, prohíbe que en la elaboración de publicidad personalizada se utilicen perfiles basados en categorías especiales de datos personales (vid. supra).

Con todo, se puede decir que se trata, por ende, de una herramienta frente a la desinformación y para defender tanto la libertad de expresión e información como la libertad ideológica⁸³. En consonancia, se persigue prevenir la difusión de contenidos ilícitos⁸⁴ o inapropiados para crear así “*un entorno en línea seguro, predecible y fiable*”⁸⁵ que proteja los derechos fundamentales de los consumidores en línea.

Para la consecución de dicho objetivo, el RSD establece una “*serie de medidas para garantizar a los usuarios mayor control sobre el uso de sus datos personales*”, y “*refuerza el principio de transparencia*”⁸⁶. También, se establecen obligaciones concretas para aquellos grandes proveedores en línea que son capaces de alcanzar un gran número de destinatarios, como son Instagram, Snapchat, TikTok o Youtube⁸⁷. Y en

⁸¹ Comisión Europea. (2024, 3 febrero). *Preguntas y respuestas...*, *Op. cit.*

⁸² *Ídem.*

⁸³ Garriga, A. (2023). Las exigencias de transparencia para los sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea en el nuevo Reglamento Europeo de Servicios Digitales. *Revista Española de la Transparencia*, 17 (Número extraordinario 2023), 137-164. p. 152

⁸⁴ La normativa no define lo que se entiende por contenido ilícito, para ello se deberá acudir a otras leyes. Comisión Europea. (2024, 3 febrero). *Preguntas y respuestas...*, *Op. cit.*

⁸⁵ Garriga, A. (2023). *Op. cit.* p. 152

⁸⁶ *Ídem.*

⁸⁷ Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, (2024). *El Reglamento de Servicios Digitales ... Op. cit.* p. 2.

especial, el RSD hace hincapié en los jóvenes y niños como usuarios en red vulnerables y que hay que proteger de todos los peligros y riesgos que existen en línea⁸⁸.

3.2.3. El reglamento de Inteligencia Artificial (RIA)

El “*AI Act*” o RIA es la primera norma de estas características aprobada a nivel mundial y responde además al compromiso adquirido por parte de la presidenta de la Comisión Europea, Ursula Von del Leyen, de crear un marco normativo basado en los valores europeos⁸⁹, los cuales se recogen principalmente en el artículo 2 del Tratado de la Unión Europea (1992).

Este Reglamento⁹⁰ tiene, en líneas generales, la estructura típica de un reglamento de gestión de los riesgos de productos industriales de cara a su introducción en el mercado de la UE. Esa estructura básica se combina, sin embargo, con la inclusión de algunas salvaguardas destinadas a la idea de crear “un ecosistema de confianza”⁹¹ mediante una normativa que no genere confusión en su uso⁹², además de respetuosa con el control de las personas sobre sus datos y la garantía de que estos últimos no serán utilizados para generar perjuicio o discriminación⁹³. Por eso se ha dicho que se trata de una normativa de carácter horizontal que regula el desarrollo de los sistemas de IA⁹⁴, aunque en consonancia tanto con la CDFUE como con el RGPD⁹⁵. Por si hubiera dudas, se destaca que este último se aplicará en todos los casos en los que se produzca “*un tratamiento de datos mediante sistemas de IA*”⁹⁶, aunque, paradójicamente en el RIA no se ha dado un lugar destacado a las agencias de protección de datos; el rol de éstas se limita al de meros

⁸⁸ Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, (2024). *El Reglamento de Servicios Digitales ... Op. cit.* p. 3.

⁸⁹ Antonov, A. (2022). Gestionar la complejidad: la contribución de la UE a la gobernanza de la inteligencia artificial. *Revista CIDOB D’afers Internacionals*, 131, 41-68.

⁹⁰ Aprobado asimismo el 21 de mayo del 2024 por el Consejo de la Unión Europea.

⁹¹ Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Generar confianza en la inteligencia artificial centrada en el ser humano*, Bruselas 8.4.2019 COM (2019) 168 final.

⁹² Sánchez, Á. A. (2020). Marco Europeo para una inteligencia artificial basada en las personas. *International Journal Of Digital Law*, 1(1), 65-77.

⁹³ Comunicación de la Comisión Europea *Generar confianza...* COM (2019) 168 final. *Op. cit.* p.5.

⁹⁴ Rincón, M. A. (2024), *Op. cit.* p. 112-113.

⁹⁵ *Íbidem*, p. 112.

⁹⁶ Cotino Hueso.L. (2024, 17 de enero). La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial. *Diario LaLey 80*, sección ciberderecho.

observadores⁹⁷ en los diferentes órganos consultivos y de control. Están pendientes, no obstante, tanto la publicación de este reglamento en el Diario Oficial, requisito imprescindible para su entrada en vigor, como más de una veintena de actos derivados de la Comisión para implementar su contenido. Entre esos actos, se espera el que dará creación a la Oficina UE de Inteligencia Artificial, con un rol muy destacado en la aplicación ordinaria del RIA.

En la elaboración del RIA ha tenido una fuerte influencia el informe que en 2019 publicó el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial. En él se recogen unas directrices éticas para una IA fiable, que no eran vinculantes por la naturaleza del informe, pero han terminado siéndolo tras su incorporación al articulado del RIA. La fiabilidad de la IA se apoya principalmente en 3 componentes que se han de satisfacer a los largo de todo el ciclo de vida del sistema (desarrollo, despliegue y utilización): (i) la IA debe de ser **lícita**, cumpliendo toda la normativa aplicable, (ii) la IA debe de ser **ética**, respetando tanto a los principios como a los valores éticos y (iii) la IA debe de ser **robusta** a fin de que la sociedad confíe en los propios sistemas y se eviten daños involuntarios⁹⁸. Por otro lado, son 7 los requisitos o principios establecidos en aras de materializar y lograr un IA fiable⁹⁹: (1) acción y supervisión humana; (2) solidez técnica y seguridad; (3) gestión de la privacidad y de los datos; (4) transparencia; (5) diversidad, no discriminación y equidad; (6) bienestar social y ambiental; (7) rendición de cuentas.

A los efectos de esta investigación tiene especial relevancia la ética en la gestión y la privacidad de los datos donde se incluye tanto “*el respeto de la privacidad, la calidad y la integridad de los datos, así como el acceso*” a los mismos¹⁰⁰. Esto es, para que un sistema de IA sea fiable, este no debe de interferir en la vida privada de las personas además de que estas deben de tener el pleno control sobre sus datos¹⁰¹, siendo ello reflejo del contenido del derecho fundamental de protección de datos personales anteriormente expuesto. Además, la protección de los datos abarcara todo el ciclo de vida del sistema

⁹⁷ Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital (s.f.). *El reglamento de IA, en resumen*. p. 8.

⁹⁸ Comisión Europea, (2019b). *Directrices éticas para una IA fiable*, Oficina de Publicaciones. p. 2 y 7-8.

⁹⁹ *Ibidem*, p. 17

¹⁰⁰ *Ibidem*, p. 18.

¹⁰¹ Nikolinakos, N. T. (2023). *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act*. Springer Nature. p. 172

de IA, lo que quiere decir que se protegen tanto los datos inicialmente facilitados por estos, como los generados a consecuencia de la interacción con el sistema¹⁰². Esto es un punto de especial relevancia sobre todo en los sistemas de IA de aprendizaje autónomo, así como en el ámbito del marketing digital, ya que los sistemas IA con los datos que se les facilita (*inputs*) pueden elaborar información (*output*) sobre tendencias del mercado entre otros, creando así una nueva categoría de datos denominados datos derivados e inferidos.

En coherencia con su enfoque basado en el riesgo, el RIA clasifica los sistemas de IA de forma jerárquica, estableciendo determinadas obligaciones y requisitos previos a la introducción en el mercado de estos sistemas¹⁰³ y a su seguimiento a lo largo del ciclo de vida¹⁰⁴. Unos pocos sistemas de IA quedan prohibidos en el artículo 5 del RIA, y se establece un régimen de muy bajo control respecto a los sistemas de IA de riesgo limitado. Consiguientemente, puede decirse que la mayor parte del articulado del RIA se destina a los llamados sistemas de **alto riesgo**¹⁰⁵ (art. 6 y siguientes RIA). Los sistemas comprendidos bajo esta modalidad se definen con carácter general en el artículo 6, procediéndose en el art. III a enumerar, en detalle, sistemas de IA que, en todo caso, han de entenderse como modalidades de alto riesgo. Este anexo III, nótese, puede ser modificado por la Comisión mediante actos delegados.

Atendiendo a la definición del art. 6 “*son componentes de seguridad de un producto, o productos sujetos a la legislación armonizada en materia de salud y seguridad de la UE*”¹⁰⁶. Encajan en esta definición, entre otros, sistemas de IA incorporados, por ejemplo, a los dispositivos médicos, los trenes o la maquinaria industrial¹⁰⁷.

A modo ilustrativo, se presenta la siguiente pirámide de riesgos:

¹⁰² Comisión Europea, (2019b). *Directrices éticas...* Op. cit. p. 21.

¹⁰³ Hupont, I., Fernández-Llorca, D., Baldassarri, S., & Gómez, E. (2024). Use case cards: a use case reporting framework inspired by the European AI Act. *Ethics And Information Technology*, 26(2).

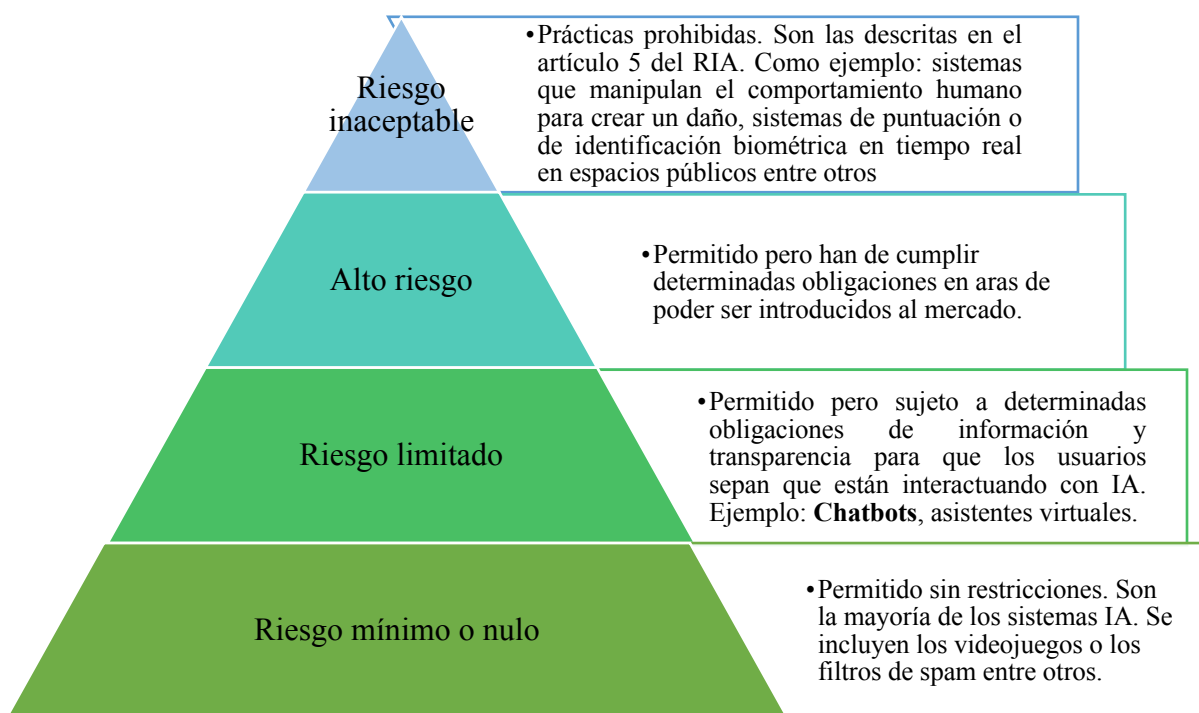
¹⁰⁴ Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital (s.f.), *op cit.* p.1.

¹⁰⁵ Que tal y como establece el Libro Blanco de la Comisión para su clasificación se tendrá en cuenta tanto lo que esté en juego como el sector y el uso y aplicación que se le den a los sistemas. Comisión Europea (2020, 19 de febrero). *Libro blanco...* Op. cit., p.21.

¹⁰⁶ Rincón, M. A. (2024), *Op. cit.* p. 119.

¹⁰⁷ Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital, (s.f.) *Op. cit.* p. 2.

Imagen 4: Jerarquía de riesgos.



Fuente: Elaboración propia a partir de Consejo de la UE¹⁰⁸

3.3. Algunas notas para tener en cuenta sobre el Paquete RDM-RSD y RIA, por cuanto afecta al marketing digital

El Paquete RDM-RSD y el RIA se elaboraron en un contexto muy particular, en el que la Unión Europea trabajaba -prácticamente contra reloj- con el objetivo de reforzar su autonomía estratégica en el proceso de transición digital. La UE busca impulsar un ecosistema de excelencia que le garantice “*estabilidad, seguridad y competitividad de los intercambios comerciales mundiales*”¹⁰⁹. Habilidades, infraestructuras, gobernanza y capacitación de empresas-personas son los ejes centrales de la *Brijuja digital* que marca el rumbo de la UE hacia el año 2030¹¹⁰, y a pesar de la insistencia en garantizar la privacidad y la protección de datos¹¹¹ no puede pasarse por alto que la UE se ve a sí misma rezagada en una carrera mundial dominada por otros. Los EEUU y China, principalmente, así como Japón o incluso Canadá están haciendo una gran inversión en investigación e

¹⁰⁸ Consejo de la UE (s.f.) *Inteligencia Artificial*.

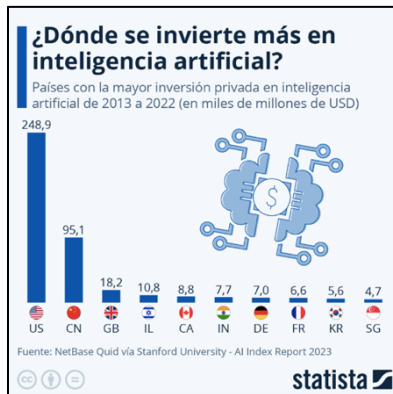
¹⁰⁹ Comunicación de la Comisión *Relativa a la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital Un mercado único digital conectado para todos*. Bruselas 10.5.2017 COM (2017) 228 final. p. 27

¹¹⁰ Comisión Europea (s.f.). *La década digital de Europa: metas digitales para 2030*.

¹¹¹ *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01)*.

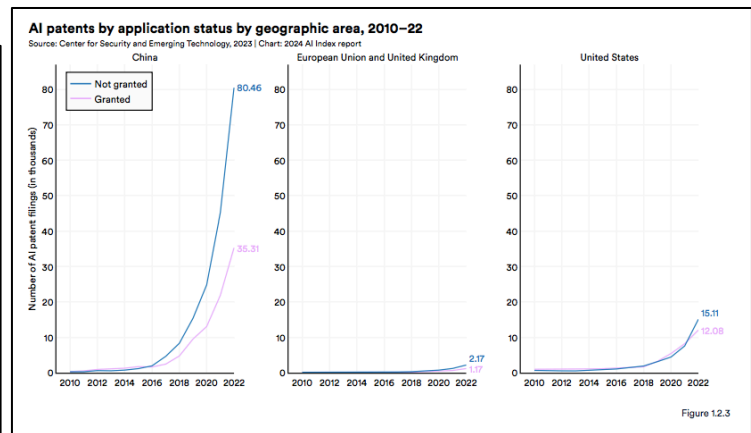
innovación y están explotando grandes cantidades de datos para poder convertirse en líderes del sector¹¹², siendo de titularidad de los EE.UU. y China la mayor parte de las patentes (véanse las imágenes 5 y 6).

Imagen 5: Inversión en IA



Fuente: Statista¹¹³

Imagen 6: Patentes IA



Fuente: Stanford University¹¹⁴

Adelantándose en la elaboración del RIA, como primer texto jurídico sobre esta materia a nivel mundial, la UE ha pretendido dos cosas: de una parte, reforzar su autonomía estratégica; de otra, garantizar un cierto “efecto Bruselas” también en este ámbito. El concepto de autonomía estratégica no es nuevo, aunque se desarrolló inicialmente en los ámbitos de seguridad y defensa. El Consejo de la UE definió el concepto de autonomía como la capacidad para actuar de forma autónoma cuando y donde fuera necesario y siempre que sea posible con sus socios¹¹⁵. Alcanzar esa autonomía respecto al uso de la IA resulta de gran trascendencia, dado que la economía de datos es considerada una de las principales fuentes de riqueza de este siglo XXI¹¹⁶. La Estrategia Europea de Datos asume como objetivos, en este sentido, los de (i) convertir a Europa en una economía capaz de manejar los datos de forma ágil y segura para así contar con la información necesaria para tomar decisiones y mejorar la vida de sus ciudadanos, y (ii) optimizar tanto

¹¹² Comunicación de la Comisión Europea. *Inteligencia Artificial para Europa*, COM (2018) 237 final. *Op. cit.* p. 5

¹¹³ Pasquali, M. (2023, 6 abril). ¿En qué países se invierte más en inteligencia artificial? *Statista Daily Data*.

¹¹⁴ Stanford University (2024). *Artificial Intelligence Index Report 20240*

¹¹⁵ Consejo de la Unión Europea (2016, 14 de noviembre). *Council conclusions on implementing the EU global strategy in the area of security and defence Foreign Affairs*.

¹¹⁶ European Union External Acton. (s.f.) *Op. cit.*

el acceso como la gestión de los datos, para que estos puedan ser reutilizados¹¹⁷. No se trata tanto de datos de carácter personal, cuanto de datos de lo más diverso que proporcionan, por ejemplo, los productos “conectados” (electrodomésticos, vehículos, teléfonos móviles, etc.) y, que, en buena medida, quedan fuera del RGPD. En cualquier caso los legisladores han subrayado que las normativas de privacidad y protección de datos mantienen plena vigencia¹¹⁸ tras la aprobación de la Ley Europea de Gobernanza de Datos, de 2023, y la Ley Europea de datos (2024), aplicable a partir del 12 de septiembre del 2025¹¹⁹. Se trata de normas Mientras que la primera de las normativas, apuesta por “*poner a disposición más datos y facilitar el intercambio de datos entre sectores y países de la UE con el fin de aprovechar el potencial de los datos*”¹²⁰, la segunda, aboga por fomentar un mercado de datos competitivo en la UE, haciendo que los mismos sean más accesible y utilizables para fomentar y favorecer la innovación. Para ello sea posible, “*garantiza la equidad en la asignación del valor de los datos entre los agentes de la economía de los datos, aclarando quien puede utilizarlos y en qué condiciones*”¹²¹.

El conjunto de textos jurídicos a los que se viene haciendo referencia a lo largo de esta investigación no tiene, además, una única intención de aplicación directa en la UE. La UE pretende que generen, de forma colateral, lo que Anu Bradford describió como “efecto Bruselas”¹²², en el sentido de “*capacidad innata de la UE (como mercado único más grande del mundo) para promulgar estándares legales globales que posteriormente sirven de inspiración y son adoptados más allá de su jurisdicción*”¹²³.

Elaborando antes que otros países sus marcos reguladores, y teniendo en cuenta que muchas de las empresas multinacionales ofrecen sus productos y servicios en la UE, ésta última pretende que sus regulaciones, aunque sea de forma indirecta, contribuyan a definir

¹¹⁷ Comisión Europea (2020, 19 de febrero). *Libro Blanco...*, *Op. cit.*, p.2-3.

¹¹⁸ Comisión Europea (s.f.). *Estrategia Europea de datos*.

¹¹⁹ La normativa entró en vigor el 11 de enero del 2024. (Gobierno de España, (2024, 12 de enero) *Entra en vigor la Ley europea de Datos estableciendo nuevas normas para una economía de datos justa e innovadora*.

¹²⁰ Comisión Europea (s.f.). *Configurar el Futuro Digital de Europa: Ley Europea de Gobernanza de Datos*.

¹²¹ Traducción propia a partir de: Comisión Europea (s.f). *Data Act explained*.

¹²² Bradford, A. (2020). *Brussels Effect: How the European Union Rules the World*, Oxford University Press. P.23-24.

¹²³ Antonov, A. (2022). *Op. cit* p.55

los estándares de funcionamiento de los negocios digitales a nivel global. Dicho de otro modo, la UE es consciente de que su rol de actora en la carreta tecnológica no está en la producción (en la que los EE.UU. y China le adelantan, como se ha visto ya) sino en su capacidad para ser determinante en las regulaciones globales¹²⁴. Ser la primera región en adoptar un marco jurídico para la IA ha sido visto, en este sentido, como un esfuerzo por garantizar que su perspectiva regulatoria será dominante en el mercado global¹²⁵. Prueba de ello, por el momento las denominadas *Big Tech* vienen aceptando aceptado las condiciones comerciales pautadas desde Bruselas¹²⁶.

Ese contexto polarizado es relevante para contextualizar algunas decisiones incorporadas a los Reglamentos que son objeto de este trabajo y evaluar la eficacia potencial de sus preceptos respecto a la protección de datos personales en el marketing digital impulsado mediante IA.

4. CASO DE USO: LONUX, comercio textil online, incorpora a su página la aplicación virtual SIRA de proveedor NIVOL

En relación con el marketing digital, si por algo destaca la IA es por su capacidad para “*acercar la oferta a la demanda*”¹²⁷, reduciendo los costes y aumentando la eficiencia¹²⁸. Todo ello, puede servir a las empresas como elementos clave a la hora de alcanzar una “*ventaja competitiva empresarial*”¹²⁹. Para ese acercamiento, sin embargo, resulta imprescindible una captación masiva de datos, tanto colectivo como personales¹³⁰.

Como aún no existe jurisprudencia que aborde supuestos de vulneración de la protección de datos en el caso que nos ocupa, se presenta a continuación el caso de uso prospectivo diseñado para testar en detalle el nivel de garantía de las normas de la UE ofrecen a la protección de datos afectada por el marketing digital.

¹²⁴ Filibi I. (2024, 24 de enero), *Op. cit.*

¹²⁵ Bradford, A. (2021, 11 enero). *The Brussels Effect Comes for Big Tech*. Project Syndicate.

¹²⁶ *Ídem.*

¹²⁷ Cuervo Sánchez, C. A. *Op. cit.*, p. 31.

¹²⁸ Huang, M. H., & Rust, R. T. , (2021) *Op. cit.*, p. 30.

¹²⁹ Medina-Chicaiza, R. P., y Martínez-Ortega, A. G., (2020) *Op. cit.*, p. 36.

¹³⁰ Stone, M., Aravopoulou, E., Ekinci, Y., Evans, G., Hobbs, M., Labib, A., Laughlin, P., Machtynger, J., & Machtynger, L. (2020). Artificial intelligence (AI) in strategic marketing decision-making: a research agenda. *The Bottom Line*, 33(2), 183-200.

4.1. Descripción del Caso de Uso

Imaginemos una empresa (**LONUX**), que se dedica a la comercialización de prendas de vestir – incluyendo ropa de diverso tipo, complementos y calzado-. Los objetivos que actualmente persigue la misma son:

- Mejorar la efectividad de sus campañas de marketing digital directo (empresa-comprador), y con ello
- Aumentar las ventas atrayendo tanto a nueva clientela, así como fidelizando también a los clientes ya existentes a través de ofrecerles productos personalizados.

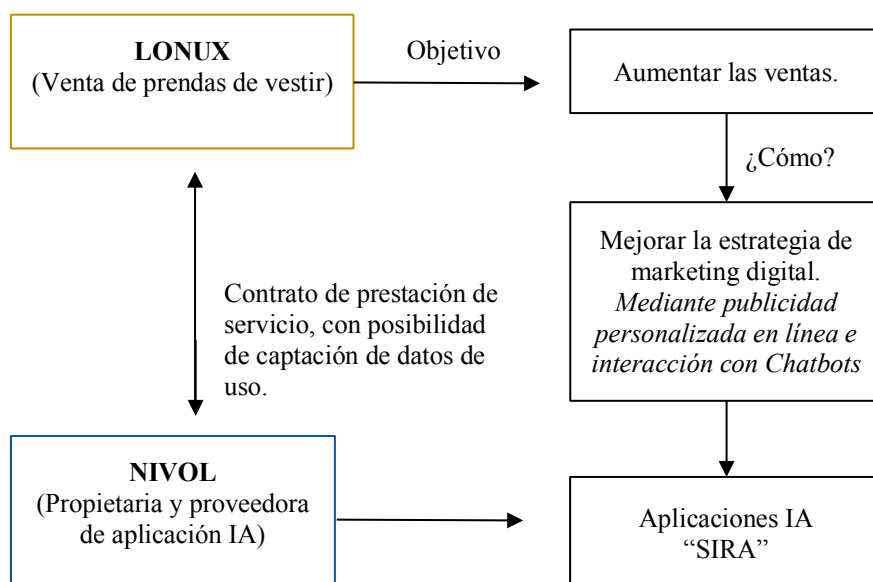
Para ello, y dado que últimamente ha escuchado mucho sobre los beneficios de las aplicaciones de IA en todas las fases de las estrategias de marketing digital, opta por innovar y utilizar técnicas avanzadas de IA para realizar un análisis predictivo que le permita conocer mejor a sus clientes actuales y potenciales, y así poder ofrecerles productos personalizados a sus necesidades y deseos.

Finalmente, LONUX decide contratar los servicios de la **aplicación SIRA** (aplicación creada y comercializada por una empresa estadounidense **NIVOL**). Esta aplicación le ofrece los siguientes servicios:

- Que los usuarios que accedan a la página web de LONUX (bien de forma identificada o no) interactúen de forma inmediata y en tiempo real a través de asistentes virtuales (Chatbots) en sus compras, los cuales son capaces de captar emociones en los rostros e inferir diferentes tipos de información de los textos que los usuarios teclean, para así ofrecerles productos relacionados con sus demandas (publicidad personalizada).
- A través de esta captación de datos y de emociones que realiza LONUX gracias a SIRA, esta es capaz mediante el correspondiente tratamiento y procesamiento de los mismos, elaborar perfiles de sus clientes. Matizar, que únicamente se podrá elaborar perfiles de clientes que se identifiquen en la web, ya que eso permitirá que los datos de compras, navegación etc. se puedan asociar a los mismos.
- Finalmente, y gracias a esta elaboración de perfiles, LONUX puede enviar publicidad personalizada a sus usuarios (vía *email marketing* por ejemplo) y mostrar publicidad programada (en base a información histórica de la propia

aplicación) que haga que sus estrategias de marketing mejores, y con ello sus ventas.

Imagen 7: Esquema 1 Caso de Uso



Fuente: Elaboración propia.

Esta aplicación (SIRA) da servicios a muchas más empresas en todo el mundo, lo que permite a sus compradores compartir un análisis predictivo¹³¹ en base a datos históricos almacenados de todas ellas. La aplicación ofrece a sus clientes por lo tanto información en base a los datos almacenados y una serie de reglas, que, mediante el aprendizaje autónomo y los nuevos datos aportados por los compradores hacen que la propia herramienta mejore y se vaya actualizando. Todo ello implica, por lo tanto, que en el contrato que han firmado ambas empresas se establece que LONUX tiene que permitir a NIVOL que obtenga **datos de uso** de la aplicación SIRA.

Como asistente virtual inteligente, SIRA comienza su funcionamiento con una serie de contenidos pre-cargados pero, **gracias a su capacidad de aprendizaje automático** (que combina *deep learning* y procesamiento natural del lenguaje) a la experiencia del uso, tiene la capacidad de ir interactuando de forma más ágil y adaptada a los potenciales usuarios. De una parte, SIRA evalúa periódicamente el rigor de las respuestas a preguntas

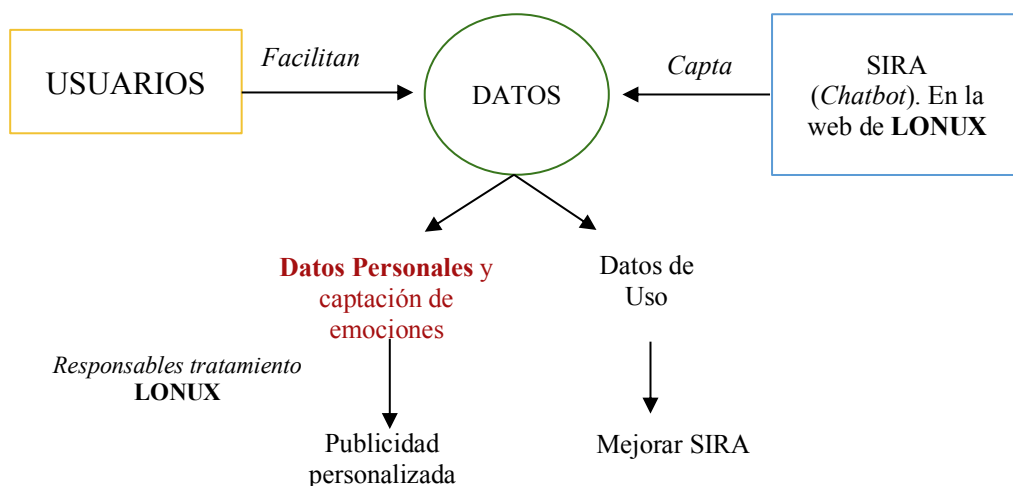
¹³¹ Ello, ofrece patrones colectivos a través de la recolección, almacenamiento y análisis de cantidad masiva de datos. Estos patrones, son clave para las empresas en aras de conocer los comportamientos de los potenciales compradores.

y de la transmisión de contenidos, agrupando todas las tipologías de dudas y las respuestas que proporcionadas en el conjunto de empresas que utilizan la aplicación.

De otra parte, SIRA es también capaz de afinar sus algoritmos a la hora de ofrecer publicidad personalizada. Su referencia en la personalización son los datos que va clasificando en conversaciones con diferentes usuarios. Al efecto, registra el recorrido de los clientes por el sitio web (para recomendarles productos similares) y, en relación con la interacción, clasifica las conversaciones con usuarios (tanto en el lenguaje procesado como en la captación de emociones), para generar categorías o perfiles de usuarios a los que, potencialmente, ofrecer productos análogos. Para su retroalimentación es asimismo importante para SIRA conocer si las lecturas que ha hecho de emociones o intenciones en las personas, en especialmente las de compra, coinciden o no con éxitos de venta. Sin revelar datos de los clientes, LONUX debe aceptar como parte del contrato de uso de SIRA su colaboración para la mejora de la aplicación, recibiendo a cambio -sin coste adicional- actualizaciones periódicas automáticas del servicio en las que se beneficia de mejoras a las que han contribuido otras empresas contratantes de SIRA.

Por lo tanto, y para que la comprensión del intercambio de datos sea más comprensible, se expone el siguiente esquema a modo ilustrativo:

Imagen 8: Esquema 2 Caso de Uso



NIVOX desde el diseño ha de garantizar que la IA es capaz de balcanizar esta información.

Fuente: elaboración propia

En este punto conviene recordar que el enfoque del presente trabajo es el análisis jurídico-constitucional de las garantías que la normativa europea ofrece, en concreto, a la protección de datos en el ámbito del marketing digital. No se tendrán en cuenta, por tanto, cuestiones que puedan ser de interés para otras áreas del derecho (como la responsabilidad civil extracontractual, la competencia desleal o la publicidad engañosa) o incluso del Derecho constitucional, como la discriminación ocasionada por los algoritmos empleados por SIRA. En concreto son cinco los elementos del supuesto de hecho descrito que encajan en los objetivos del presente trabajo:

1. La compra por parte de una empresa con sede en la UE (LONUX) a una empresa de EEUU (NIVOL) de los servicios de una aplicación con IA (SIRA) y de la clasificación de dicho sistema en la jerarquía de riesgos de RIA, así como de las obligaciones de las partes.
2. La captación de datos a través de la interacción con los asistentes virtuales (SIRA).
3. El tratamiento automatizado de datos personales que realiza LONUX a través de SIRA para poder ofrecer publicidad personalizada a los usuarios.
4. El complemento a la de protección de datos que ofrece el RSD.
5. De los mecanismos que tienen los usuarios para proteger su derecho fundamental a la protección de datos

4.2. De la compra y puesta en el mercado de la UE de la aplicación SIRA (de proveedor estadounidense), para su uso por LONUX

Dado que se trata de una aplicación de IA que va ser implementada en la UE y que posibilita la captación de datos personales para ser empleados en la mejora de las estrategias de marketing digital, son objeto de análisis en este apartado tanto el RGPD como el RIA. En primer lugar, se analizarán los ámbitos de aplicación y las partes implicadas en el caso de uso, para posteriormente definir de qué tipo de sistema de IA se trata la aplicación SIRA y por lo tanto qué obligaciones se han de seguir para poder comercializarla en la UE.

4.2.1. La cuestión de la territorialidad de la aplicación SIRA a los efectos de la aplicación de RGPD y el RIA

Tal y como se ha expuesto, estamos ante la compra por parte de una empresa de la Unión Europea (LONUX) a una empresa (NIVOL) de un tercer país (EE.UU.) de una aplicación de IA. El primer punto a destacar es que, si bien es cierto que el **RIA** es una normativa europea, su ámbito de aplicación es mucho más amplio. La misma, se aplica a:

- i. Los **fabricantes y proveedores (NIVOL)**, entendidos como las personas físicas o jurídicas que desarrollan un sistema de IA y que lo comercializan o lo ponen en servicio en el mercado interior de la Unión (art. 3 RIA), independientemente de que los mismos estén establecidos o no en la Unión (art. 2 RIA). En este caso de trata de una empresa estadounidense. Será la responsable de tramitar la puesta en mercado de SIRA y por lo tanto saber de qué tipo de IA basada en el riesgo se trata.
- ii. Los **implementadores** de estos sistemas (**LONUX**), que son las personas físicas o jurídicas que utiliza un sistema de IA bajo su autoridad (art. 3 RIA), y que tengan su lugar de establecimiento en la unión (art. 2 RIA).

Esta extensión del ámbito de aplicación territorial es reflejo una vez más de que tal y como se estipuló en el Libro Blanco de la Comisión, por un lado, se quiere un “*alcance geográfico de intervención legislativa*” que traspase las fronteras de la Unión aplicándose la misma a todos los agentes económicos que ofrezcan este tipo de sistemas¹³², y por otro lado, se pretende regular todo el ciclo de vida¹³³ del sistema de IA, así como establecer obligaciones a todas las partes intervinientes en el mismo, teniendo en cuenta quien se encuentra en “*mejor posición para abordar todo posible riesgo*”¹³⁴.

En lo que al **RGPD** concierne, este se aplica a:

- i. Los **responsables**, que son quienes fijan los fines y medios de tratamiento¹³⁵ (art. 4 RGPD). En el presente caso se trata de **LONUX**, ya que es quien haciendo uso

¹³² Comisión Europea (2020, 19 de febrero). *Libro Blanco... Op. cit.*, p.27.

¹³³ Las fases de un sistema IA son: i) la planificación y el diseño, ii) la comprobación y la validación; iii) el despliegue y iv) el funcionamiento y el seguimiento. (OECDiLibrary. (s.f.). *La inteligencia artificial en la sociedad*. Dado que en el presente caso de uso nos encontramos en la puesta en marcha del servicio, nos vamos a ceñir al uso de datos personales que se da en esa fase del ciclo de vida del sistema de IA.

¹³⁴ Comisión Europea (2020, 19 de febrero). *Libro Blanco... Op. cit.*, p.27.

¹³⁵ Como se ha expuesto en el apartado *supra* 3.2.1, el tratamiento de datos engloba diferentes acciones entre las que se encuentran: la recogida de datos, estructuración, conservación, adaptación, utilización y comunicación. Todo ello es lo que capaz de hace la aplicación de IA SIRA.

de los servicios de la aplicación SIRA recopila y trata la información necesaria de los usuarios de su página web para mejorar su estrategia de marketing digital.

No se puede dejar de lado una de las notas características de los sistemas de IA, el hecho de que los mismos se siguen desarrollando y se mejoran a través de los datos que se le introducen (*inputs*). Esto es, SIRA es capaz de ofrecer información sobre tendencias en el mercado (*outputs*) (que posteriormente puede emplear LONUX para ofrecer publicidad programada), e información personalizada de los usuarios a LONUX (*outputs*); pero ha de generarse una barrera (para cumplir de forma voluntaria, aunque aún no sean obligatorias, las previsiones del Reglamento de Servicios Digitales) respecto a NIVOL.

NIVOL, como prestadora del servicio de SIRA, tiene derecho a datos de uso (no personales) que mejoren el funcionamiento de la aplicación. Una parte de esos datos los maneja autónomamente SIRA que es capaz de aprender -se ha dicho ya-. Tanto esos datos autónomamente gestionados como otros que capte NIVOL con fines de mejora de la aplicación generan responsabilidades para NIVOL, porque sira, como es obvio, no tiene personalidad jurídica. NIVOL no está autorizada para emplear datos personales de los usuarios de SIRA que acceden a ella mediante LONUX. Es más, la normativa le obliga a que como proveedor de SIRA se asegure de que existen barreras técnicas que delimitan con seguridad suficiente los datos personales respecto a los datos de uso. Es por esta razón, por la que en el presente supuesto de hecho y en relación al ámbito de aplicación personal del RGPD NIVOL no tiene en sentido estricto condición ni de responsable ni de encargada.

RIA	RGPD
<p>LONUX: Implementadora</p>	<p>LONUX: Responsable (Fase de despliegue) Responsable de la protección de los clientes y usuarios de su Chatbot (SIRA)</p>
<p>NIVOL: Fabricante y proveedora Será la responsable de los requisitos de seguridad del sistema.</p>	<p>NIVOL: No está legitimada para acceder a los datos de las personas usuarias del asistente virtual que funciona, en concreto, en la web de LONUX. Se debe generar una barrera sólida (la debe generar NIVOL; porque LONUX no tiene acceso a los mecanismos de SIRA) donde se separen, por un lado, los datos de uso y por otro lado los datos personales. Con todo, el diseño de la política de privacidad que puede ofrecer LONUX como usuario de SIRA depende de NIVOL.</p>

Se mantiene de este modo el objetivo de la Ley Europea de Datos de 2024, tendente a facilitar el intercambio de datos de uso entre empresas (B2B¹³⁶), pero sin que *“ninguna disposición del presente Reglamento debe aplicarse o interpretarse de manera que se reduzca o limite el derecho a la protección de los datos personales¹³⁷”*. En cualquier caso, siguiendo las recomendaciones de la AEPD y teniendo en cuenta la complejidad de estos tipos de uso, es importante reducir *“el riesgo de que la “responsabilidad” se diluya o se presenten asimetrías en el nivel de cumplimiento de cada una de las partes¹³⁸”*.

4.2.2. La clasificación de “SIRA” en las modalidades de riesgo del RIA y sus implicaciones para la protección de datos

Una vez detalladas las partes intervinientes, en este apartado se procede a analizar dentro del RIA en qué categorización del riesgo se enmarcaría la aplicación SIRA, que tal y como se ha expuesto, será NIVOL (proveedora) la encargada de categorizarlo.

El sistema IA SIRA, gracias a los asistentes virtuales, ayuda a la LONUX en la toma de decisiones mediante el tratamiento y procesamiento de datos personales a través de la elaboración de perfiles gracias a la captación de las emociones y del teclado de sus usuarios. Ello, hace que se mejoren sus estrategias de marketing digital (y sus ventas), ya que puede ofrecer publicidad personalizada y programada a sus usuarios optimizando así su experiencia de compra.

Tal y como se ha expuesto en la jerarquía de riesgo (Ver Imagen 4), este tipo de los asistentes virtuales, en aplicación de lo ya descrito respecto al art. 6 RIA y el Anexo III, serán considerados sistemas IA de **riesgo limitado**. Por ello y a pesar de que los mismos afectan de forma más restringida a los derechos y libertades de los usuarios, los proveedores siguen teniendo que cumplir determinadas obligaciones a fin de asegurar un entorno en línea más seguro. En concreto, la obligación de la NIVOL se traduce a determinadas obligaciones de transparencia como es poner en conocimiento de los usuarios que los mismos están en contacto/interactuando con una aplicación de IA (art 50 RIA). A ello, le es de aplicación una excepción, ya que no será necesaria que las

¹³⁶ *Business to Business*

¹³⁷ Considerando 7º Ley Europea de Datos

¹³⁸ AEPD (2020, 3 de diciembre) *IoT (I): Qué es IoT y cuáles son sus riesgos*. AEPD.

“personas estén informadas cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz que están interactuando con un sistema de IA, teniendo en cuenta las circunstancias y el con texto de la utilización”. Asimismo, al tratarse SIRA de un sistema capaz de reconocer emociones, los responsables del despliegue (tanto proveedores como implementadores) deben informar *“a las personas físicas expuestas al mismo del funcionamiento del sistema y se tratarán los datos personales de conformidad”* con el RGPD (art. 50.3 RIA).

La clasificación de SIRA como IA de riesgo limitado tiene importantes consecuencias en términos de garantías para los usuarios finales. Sus proveedores e implementadores no requieren conforme al RIA una evaluación de riesgo previa a la implementación, y el ciclo de vida de estos sistemas queda sometido, básicamente a los códigos de conducta que, de forma voluntaria, NIVOL y/o LONUX deseen asumir.

4.3. La captación de los datos de los usuarios en la interacción con el *Chatbot* de SIRA: datos personales y reconocimiento biométrico de emociones

Tal y como se ha expuesto, la captación de datos personales se da en el momento de interacción con el asistente virtual SIRA. Aclarar, que únicamente serán datos personales a efecto de protección por el RGPD los datos de los usuarios que interactúan con SIRA tras haberse identificado en la página web. De no ser así y de interactuar con el *chatbot* como un simple “visitante” en la página web estos datos no podrán ser asociados o utilizados para identificar a un usuario, y por lo tanto no estarán bajo la salvaguarda del reglamento.

Asimismo, lo que sucede con la IA es que, si bien la misma se alimenta la de información que se le proporciona (*inputs*), la misma también es capaz de crear y generar nuevos datos (*outputs*). Por lo que son distintos tipos de datos los que se han de tener en consideración a fin de su protección. Por si ello no fuera suficiente, en el contrato que han firmado ambas empresas, se estipula que NIVOL tiene posibilidad de captar datos de uso en sentido estricto.

En primer lugar, y en aplicación del principio de licitud que impone el RGPD, todo tratamiento ha de tener una base jurídica, bien porque el usuario ha dado su consentimiento (que en base al RGPD deberá de ser inequívoco), bien porque existe un

interés legítimo siempre que no prevalezcan los derechos fundamentales sobre el mismo¹³⁹. En lo que al interés legítimo del responsable del tratamiento se refiere, el considerando 47º del RGPD establece que “*el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo*”. Por lo tanto, se observa como el uso de datos personales dentro de la esfera del marketing digital puede verse justificado sin la necesidad del consentimiento de los interesados. Ello, sin duda, hace que la protección de los datos personales de los mismos se vea reducida.

Los usuarios, muchas veces pueden ser conscientes de que los mismos están consintiendo el tratamiento de sus datos personales (datos facilitados). Ahora bien, puede que desconozcan que también existe la posibilidad de que se estén tratando datos personales derivados, que son aquellos que se “*obtienen a través del procesamiento de los datos facilitados*” o datos inferidos, aquellos “*obtenidos a partir del procesamiento analítico de un conjunto amplio de datos entre los que se encuentran datos de múltiples personas usuarias y diversas fuentes*¹⁴⁰”.

En el caso objeto de análisis, encontramos que se dan todos esos tipos de datos:

- Datos facilitados: aquellos datos que facilitan conscientemente los propios usuarios cuando interactúan con SIRA y, si lo desean, cuando se identifican en la página web de LONUX. En este caso, al tratarse de una tienda de ropa, se parte desde el correo electrónico que ha podido aportar la usuaria junto con su nombre, así como la talla de ropa que le facilita a SIRA a fin de que le ofrezca proyectos que encajen con sus necesidades. EL RGPD, en cualquier caso, obliga a que las personas tengan la opción de realizar compras como invitadas, sin registrarse, caso en el que actuarán como anónimas ante SIRA.

- Datos biométricos relativos a las emociones. En este apartado, se ha de hacer una mención separada del reconocimiento de emociones que realiza SIRA. Como se ha dicho ya, el RGPD define como biométricos aquellos datos que, mediante algún proceso técnico, se han obtenido de las características anatómico-físicas, fisiológicas o comportamentales de las personas, pero siempre y cuando sirvan

¹³⁹ AEPD. (2020, febrero). *Adecuación al RGPD...*, Op. Cit.p. 21.

¹⁴⁰ AEPD (2020, 3 de diciembre). *IoT (I): Qué ... Op. Cit.*

para confirmar la identidad única de una persona (art. 4.14. RGPD). Las biometrías que captan emociones, en cambio, son datos no singularizantes. A los efectos del RIA, sin embargo, la captación de emociones es muy relevante y, por ello, en su art. 3.34 el RIA ofrece una noción de datos biométricos diferente a la del art. 4.14 RGPD. Se puede decir que al amparo del RGPD, las emociones captadas de los usuarios serán categorizadas dentro de los datos personales generales únicamente cuando esos datos hayan sido captados y tratados como vinculados a una persona identificada o identificable.

- Datos derivados: aquellos datos que, a través del correspondiente tratamiento, emplea LONUX para conocer las preferencias de sus usuarios. Se está por lo tanto de una elaboración de perfil que posteriormente se emplearía para diseñar publicidad personalizada.
- Datos inferidos: aquellos datos de un conjunto amplio de usuarios que trata LONUX para conocer tendencias de mercado y consumo.

Por lo tanto, cabe preguntarse si cuando se da el consentimiento de tratamiento de datos personales (hecho que lo legitima), se está dando también el consentimiento para el tratamiento de la información que ha sido generada a través de esos datos. Sin una disposición clara al respecto, lo que sí podemos anunciar es que en estos casos y tomando el RGPD como base de análisis, entra en juego uno de los principios de todo tratamiento de datos como es la **limitación del fin establecido**. Esto es, el tratamiento se debe ceñir a *“aquellos fines determinados, explícitos y legítimos que se hayan identificado¹⁴¹”*. Esto está en perfecta consonancia también con el principio de **minimización** de datos, donde se emplearán únicamente aquellos datos necesarios para el fin establecido. Esto es, únicamente se accederá a esos datos cuando sea necesario y cuando se demuestre que se necesita usarlos.

A todo ello se le suma también el principio de **información y transparencia**, de modo que conforme a la normativa vigente los usuarios deben tener en conocimiento de: (1) que el asistente virtual que utiliza LONUX, es un asistente virtual al que da soporte NIVOL; (2) que SIRA puede captar datos personales que serán utilizados con fines de

¹⁴¹ AEPD. (2020, febrero). *Adecuación al RGPD...*, Op. Cit.. p. 21.

marketing por LONUX; (3) que no se grabará su imagen, pero que sí se extraerá de su rostro información biométrica destinada a interpretar sus emociones.

Finalmente, y en relación al uso que NIVOL hará respecto a datos que le permitan evaluar el funcionamiento de SIRA y, en su caso, actualizarla y mejorarla, NIVOL podrá ser requerido para demostrar que a este respecto SIRA únicamente maneja datos siempre anonimizados (de forma irreversible), sin margen para que pueda producirse una reidentificación¹⁴².

4.4. El tratamiento automatizado de datos personales que realiza LIXUS a través de SIRA para poder ofrecer publicidad personalizada a los usuarios.

Si un componente IA realiza tratamiento de datos personales, elabora perfiles sobre una persona física o si toma decisiones sobre la misma, tendrá que someterse al RGPD¹⁴³. Esto, es en concreto lo que sucede con la aplicación SIRA, quien a través de los datos captados en la interacción usuario-asistente virtual, elabora patrones que permiten a LONUX realizar una publicidad personalizada que haga que sus ventas puedan verse incrementadas.

Tal y como se ha expuesto en el apartado 4.2.2 *supra*, el RIA no considera, de primeras, de alto riesgo estos sistemas de IA y deja su protección en el RGPD. Se entiende por elaboración de perfil a *“toda forma de tratamiento de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos a (...) preferencias personales”* (art 4.4 RGPD). Además, se debe tener en consideración que en base al artículo 22 del RGPD ningún interesado¹⁴⁴ debe de ser objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos¹⁴⁵, donde se incluye la elaboración de perfiles, que produzca efectos jurídicos o le afecte significativamente.

¹⁴² AEPD. (2020, febrero). *Adecuación al RGPD...*, *Op. Cit.* p. 14.

¹⁴³ *Ídem*.

¹⁴⁴ El RGPD hace referencia a través de este término a la persona cuyos datos personales están siendo tratados.

¹⁴⁵ Son aquellas decisiones realizadas por medios tecnológicos sin la intervención humana. (AEPD. (2020, febrero). *Adecuación al RGPD...*, *Op. cit.* p. 10).

En este punto, cabe reflexionar sobre la siguiente cuestión: ¿la realización de publicidad personalizada (decisión que toma LONUX gracias a la elaboración de perfil realizada por SIRA) basada únicamente en el tratamiento de datos queda amparada por la presente disposición? Si bien es cierto que no existe Jurisprudencia al respecto al tratarse una materia muy reciente, el pronunciamiento del TJUE del pasado 7 de diciembre del 2023 puede servir para orientarnos en dicha cuestión. En la sentencia, se entiende por “**decisión individual automatizada**” a la generación de un valor de probabilidad de una entidad (SIRA) si el mismo influye de manera determinante en la decisión de un tercero (LONUX)¹⁴⁶. Esto se debe a que, según el TJUE, el concepto de decisión “*no se refiere solo a actos que produzcan efectos jurídicos que afecten al interesado de que se trate, sino también a actos que lo afecten significativamente de modo similar*”¹⁴⁷.

Se observa como el TJUE aboga por una concepción garantista del término decisión, donde tanto el responsable formal como el encargado que procesa los datos llegan a tener obligaciones¹⁴⁸. Además, esta sentencia sirve para aportar luz y poner el foco en la influencia que tienen los resultados obtenidos por IA en la decisión final automatizada por quienes lo usan y, por lo tanto, en su posible consideración de sistema de alto riesgo¹⁴⁹. Aún así, el simple hecho de estar ante un tratamiento de datos automatizado no es suficiente, al igual que sucede en el RIA, se tiene que seguir probando el hecho de que esta decisión afecte significativamente a los DERECHOS FUNDAMENTALES de los usuarios, labor compleja en el entorno del marketing digital y publicidad, donde entran en conflicto derechos como la libertad cognitiva de los compradores y la libertad de empresa de los vendedores.

Ahora bien, pesar de que el RGPD deja sin definir este término, las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 elaboradas por el Grupo de Trabajo sobre Protección de Datos del art 29, establece que en determinadas ocasiones es posible que **la publicidad en línea sí pueda tener un efecto significativo en los usuarios**, pero como suele suceder habrá de hacer una ponderación atendiendo a las circunstancias especiales de cada caso¹⁵⁰. A modo ejemplificativo se exponen las siguientes características que podrán ser valoradas a fin de

¹⁴⁶ Cotino Hueso.L. (2024, 17 de enero). *Op. Cit.*

¹⁴⁷ Apartado 44, STJUE C 634/2.

¹⁴⁸ Cotino Hueso.L. (2024, 17 de enero). *Op. Cit.*

¹⁴⁹ Ídem.

¹⁵⁰ Grupo de trabajo sobre protección de datos del artículo 29 (2018, 6 de febrero). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679.*

determinar el alcance dicho concepto: *“la forma en la que se presenta el anuncio, las expectativas y deseos de las personas afectadas, el nivel de intrusismo del proceso de elaboración de perfiles o el uso de conocimiento sobre las vulnerabilidades de los interesados¹⁵¹”*.

Asimismo, no se puede dejar de lado el hecho de que corresponde a los responsables del tratamiento, gestionar el riesgo que pueda ocasionar dicho tratamiento tanto para los derechos como las libertades de los usuarios¹⁵² (art 32 RGPD). Ello, se enmarca en concreto dentro del principio del RGPD, como es el **principio de “Responsabilidad proactiva”**. En especial, se habrá de hacer una Evaluación del Impacto de la Privacidad previa *“cuando se realice la elaboración de perfiles, basados en tratamientos automatizados¹⁵³”*. Por ende, se habrá de confiar en el buen actuar de los responsables, en este caso de LONUX, al analizar el impacto que puede llegar a tener SIRA en los datos personales de sus usuarios.

Finalmente, si bien es cierto que la decisión última en este caso la toma un ser humano (LONUX), puede existir el denominado *“sesgo en la interpretación de los resultados”*, donde sin valoración crítica se adaptan como ciertos los resultados aportados por la IA¹⁵⁴. Por lo tanto, ¿qué diferencia existe en que la decisión sea tomada automáticamente por un sistema IA o por un ser humano que da por correctos sus resultados? Lo que se puede dilucidar es que los principios éticos en los que se deberían de basar los sistemas IA según el Grupo de los Altos Expertos, entre los que se encuentra la supervisión humana, no se cumplen. Dejando en entre dicho el pilar fundamental en el que se debía de basar la normativa, el generar un **entorno de confianza** para sus usuarios.

4.5. Impacto que tiene en la protección de datos el hecho de que SIRA sea un “Servicio Digital” que proporciona y mantiene NIVOL respecto a múltiples usuarios

El RSD tiene unos objetivos muy concretos, como son: *“(i) Proteger a los usuarios frente riesgos de internet, (ii) Evitar la venta de servicios, bienes o publicación de contenidos ilegales, (iii) Combatir la desinformación y la publicidad engañosa, (iv) Someter a los*

¹⁵¹ Grupo de trabajo sobre protección de datos del artículo 29 (2018, 6 de febrero). *Op. Cit.* p. 24.

¹⁵² AEPD. (2020, febrero). *Adecuación al RGPD...Op. Cit.* p. 30

¹⁵³ *Íbidem*, p. 31

¹⁵⁴ *Íbidem*, p. 8.

*prestadores de servicios a auditorías independientes, incluyendo garantías para la protección de menores y (v) Limitar el uso de datos personales sensibles con fines publicitarios”.*¹⁵⁵

Por lo tanto, en lo que al caso de uso se refiere, el mismo, al igual que el RGPD introduce dos restricciones respecto a la publicidad personalizada. De un lado, prohíbe aquella publicidad personalizada dirigida a menores elaborada a través de perfiles (en línea con el RGPD) (art 28.2 RSD) y también aquella elaborada utilizando categorías especiales de datos (los cuales vienen definidos en el artículo 9 del RGPD), independientemente de que se trata de un menor o no (considerando 69º art 26.3 RSD)¹⁵⁶.

Se observa, por lo tanto, que, al tratarse de un reglamento con objetivos concretos, la protección de datos se deja una vez más a la esfera del RGPD. Además, y en lo que a la personalización de la publicidad se refiere, se tienen únicamente en consideración tanto las personas como los datos más sensibles y vulnerables. Por lo tanto, si se analiza en consonancia con el propio RGPD, donde la elaboración de perfiles de forma automatizada ha de contar con una afección significativa a los DERECHOS FUNDAMENTALES de las personas, se observa como ninguno de los dos reglamentos ofrece salvaguardas específicas para los datos personales en el ámbito del marketing digital, ni tampoco podemos considerar que aquellas garantías que ofrecen de forma genérica y son aplicables al caso resultan suficientes. Ante la IA y los servicios digitales, incluso tras aprobación de los nuevos instrumentos jurídicos, el RGPD, a pesar de sus carencias, es la normativa más garantista de cuantas están en vigor.

4.6. Mecanismos que los usuarios finales de SIRA en el comercio online de LONUX tienen para proteger su derecho fundamental a la protección de datos

Finalmente, cabe analizar con qué mecanismos cuentan los usuarios para poder salvaguardar sus datos personales en el marketing digital impulsado por IA. Anteriormente se ha expuesto que el derecho fundamental de protección de datos personales lo que hace es ofrecer a los usuarios un control sobre los mismos, por lo tanto, en tanto en cuanto dicho control se vea suficientemente garantizado, el mismo, en

¹⁵⁵ LetsLaw. (2024, 17 mayo). *Reglamento de Servicios Digitales, ¿cuál va a ser su impacto?*

¹⁵⁶ Comisión Europea. (2024, 3 febrero). *Preguntas y respuestas... Op. cit.*

principio, no se considera vulnerado. Este control, se desarrolla a través del abanico de diferentes derechos que se recogen en el RGPD. En concreto, se trata de los mencionados en el apartado 3.1 *Supra*.

No obstante, de especial relevancia es en el ámbito del marketing digital el denominado **derecho de oposición** (art 21.2 y art 21.3 RGPD¹⁵⁷), donde se establece que los interesados tienen derecho a solicitar que sus datos no sea utilizados para fines específicos tales como el marketing directo. Los mismos, pueden oponerse al tratamiento de sus datos, donde se incluye de elaboración de perfiles anteriormente expuesta, cuando el objeto del tratamiento sea la mercadotecnia directa. Aquí, una vez más, entra la obligación de **transparencia** por parte de los responsables de tratamiento de informar a los usuarios del fin de sus datos.

Ahora bien, siempre y cuando dichas herramientas de control no fueran suficientes o no estuviesen garantizadas mediante mecanismos y procedimientos adecuados por parte del responsable del tratamiento¹⁵⁸, y los usuarios/interesados considerasen que ha visto vulnerado su Derecho Fundamental a la protección de datos, tendrían abierta la vía jurisdiccional ante diferentes Tribunales.

5. CONCLUSIONES

1. El constitucionalismo digital es un término acuñado para hacer referencia al esfuerzo de adaptar y aplicar los principios del constitucionalismo tradicional a la era digital. En expresión de Balaguer Callejón, las reglas que se aplican al espacio digital han surgido al margen de los mecanismos garantistas de los Estados, y se hace necesario buscar nuevos paradigmas que permitan extender a esos dominios el respeto que merecen los derechos y las libertades fundamentales. En esa búsqueda se han dado importantes pasos por parte de la Unión Europea, pero la tarea no puede darse aún por terminada.

¹⁵⁷ En el mismo sentido el considerando 70º del RGPD “*Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información*”.

¹⁵⁸ AEPD. (2020, febrero). *Adecuación al RGPD... Op. Cit* p. 24.

2. Las aspiraciones de este constitucionalismo digital en la UE se ven, de algún modo, condicionadas por otros objetivos que se persiguen en términos socioeconómicos y de impulso de la innovación. En una realidad donde el mercado ha sido y es clave para el desarrollo de la Unión, no ha primado el principio *pro libertate*, rebajándose así la salvaguarda de los DERECHOS FUNDAMENTALES de las personas a favor de la innovación y la prosperidad del mercado interior de la Unión. Esto se debe a que la UE sabe que, para poder ser un actor influyente a escala internacional, su mercado también lo tiene que ser, por ello, debe de dejar espacio y ser flexible para que el mismo evolucione y se desarrolle.

3. A pesar de lo advertido en el punto anterior, es conveniente destacar la importante labor que han realizado los legisladores europeos a fin de haber alcanzado diversos consensos normativos en un tiempo récord. Aunque estos no son todo lo garantistas que hubiera sido deseable, marcan la hoja de ruta a seguir por parte de las instituciones comunitarias y los Estados Miembros. Por su parte, el marco normativo actual de protección del derecho fundamental de protección de datos en el marketing digital impulsado por IA tampoco es el ideal y presenta algunas lagunas, siendo ello reflejo de que las autoridades son conscientes de las necesidades que tenemos a medio y largo plazo. Sin embargo, se puede decir que, teniendo una base normativa, es más sencillo llevar a cabo modificaciones posteriores de la misma que comenzar desde cero.

4. Esta labor normativa que formaba parte de la estrategia digital europea, ha hecho que la Unión se convierta en un actor influyente en cuando a su regulación. Por lo contrario, y a pesar del posible “efecto Bruselas”, se ha de notar el hecho de que la UE queda fuera de la carrera digital liderada por EEUU y China. Lo que significa también, que siempre y cuando estos dos actores internacionales sigan siendo quienes ostentan la propiedad de las patentes de los sistemas de IA que se comercializan en el mercado de la UE, seguirán siendo también quienes mayor almacenamiento de datos alberguen con el valor estratégico que ello supone.

5. El estatuto jurídico del marketing digital impulsado por IA queda un tanto fragmentando, con solapamientos en determinadas cuestiones y con elementos que no se han atendido adecuadamente. Y si bien una normativa horizontal correspondiente a dicha materia hubiera sido un escenario ideal, la realidad es muy distinta, y se han de conjugar

varias normativas con objetivos diferentes a fin de salvaguardar los datos personales en dicho ámbito.

6. Tras haber realizado un exhaustivo análisis al respecto, se ha determinado que son tres principalmente los textos normativos que contienen las claves del derecho fundamental de protección de datos personales en el marketing digital impulsado por la IA: RGPD, RSD y RIA. Ninguno de ellos resulta específico ni recoge la cuestión de forma global. De los tres textos, por su parte, es el RGPD el que, sin ser perfecto, ofrece garantías más tangibles. El RIA y el RSD, por su parte, se extienden sobre aspectos complementarios que el RGPD no supo anticipar, pero se trata por lo contrario de Reglamentos más débiles e imprecisos en lo que se refiere a las salvaguardas para los derechos de las personas.

7. Por cuanto se refiere a las previsiones del **RGPD** aplicables al marketing digital impulsado mediante IA son varias las lagunas existentes. Por un lado, el hecho de no categorizar los datos biométricos de captación de emociones como de categoría especial rebaja su salvaguarda, al mismo tiempo que se hace complicado probar en este ámbito que un tratamiento de datos automatizado afecta “*significativamente*” a los DERECHOS FUNDAMENTALES de los usuarios. Ahora bien, fue un acierto por parte de los legisladores apostar por una normativa con mayor rango que una Directiva y de obligado cumplimiento para todos los EEMM a fin de crear un entramado normativo armonizado y garantista.

8. Por cuanto se refiere a las garantías que, en el espacio del marketing digital, aporta el **RSD**, el mismo se limita a establecer las mismas obligaciones que el RGPD en lo que a la publicidad personalizada se refiere. El **RIA**, por su parte, es un reglamento realizado en un contexto muy específico. Se trata de un reglamento a prueba de futuro y que además cuenta todavía con un amplio margen de mejora, algo que da que confiar en que determinadas disposiciones serán modificadas a fin de ofrecer mayores garantías. En concreto, en lo que al marketing digital se refiere, al igual que sucede en el RGPD se ha de probar que los DERECHOS FUNDAMENTALES están afectados “*significativamente*” para que los sistemas IA cuenten con la categoría de alto riesgo y por lo tanto con un mayor control para su puesta en marcha en el mercado de la Unión. Además, el RIA, en todo lo que a la protección de datos se refiere deja paso el RGPD. Por lo tanto, se puede entender con una normativa *lex specialis* que en caso de contradicción o duda con el RGPD sería esta última la que primaria. Tampoco se puede

dejar de lado que, dada la opacidad (IA de caja negra) e imprevisibilidad que caracteriza a determinadas acciones de la IA, muchas veces no es posible encontrar el motivo subyacente a determinadas decisiones, siendo por lo tanto complicado comprobar que la normativa se está aplicando adecuadamente con la inseguridad jurídica y pérdida de confianza de los ciudadanos que ello supone.

9. Con todo, en este entramado normativo, se ha de destacar también el papel clave que tienen las Agencias de Protección de Datos como instituciones vinculadas al RGPD. Se trata de un elemento esencial a fin de salvaguardar la protección de datos personales de los usuarios ante una hipotética vulneración en un escenario del marketing digital impulsado por IA. Esto es, a la ya garantía ofrecida tanto por la normativa como por los tribunales, se le suma la protección que se ofrece desde estas instituciones, que, en determinadas ocasiones, pueden suplir la carencia de las otras vías de garantía, al encontrarse además más al alcance de los ciudadanos.

10. Finalmente, y transcribiendo las palabras de la presidenta de la Comisión Europea, Ursula von der Leyen, en su Discurso sobre el Estado de la Unión de septiembre de 2020 "*El futuro será lo que de él hagamos. Y Europa será lo que queramos que sea*". Por lo tanto, confiemos en que se siga trabajando por un futuro en el que los DERECHOS FUNDAMENTALES estén debidamente protegidos ante la IA.

6. RECONOCIMIENTOS

El presente TFG es parte de la investigación llevada a cabo por la autora dentro del grupo de Investigación de la UPV-EHU en el seno del proyecto *AI-Biosurv, Biovigilancia mediante IA en la Era PostCovid*, financiado el mismo por los fondos *NextGenerationEU* de la Unión Europea (IPs: L. Escajedo San-Epifanio y F. Balaguer Callejón). La autora ha podido ser partícipe de dicho grupo gracias a la concesión de una de las becas que ofrece el Gobierno Vasco de investigación IKASIKER 23/24.

7. BIBLIOGRAFÍA Y REFERENCIAS DOCUMENTALES

7.1 Bibliografía

- Agencia Española de Protección de Datos (2020, 3 de diciembre) *IoT (I): Qué es IoT y cuáles son sus riesgos*.
- Agencia Española de Protección de Datos (2023, 11 de noviembre). *Protección de datos por defecto*. <https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/proteccion-de-datos-por-defecto>
- Agencia Española de Protección de Datos (2024, 8 de marzo). *Derechos y deberes*. <https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos/derecho-de-acceso>
- Agencia Española de Protección de Datos (s. f. a). *¿Cuáles son las bases de legitimación para el tratamiento de datos?* <https://www.aepd.es/preguntas-frecuentes/2-rgpd/5-bases-juridicas-de-los-tratamientos/FAQ-0214-cuales-son-las-bases-de-legitimacion-para-el-tratamiento-de-datos>
- Agencia Española de Protección de Datos (s. f. b). *Derecho a no ser objeto de decisiones individuales automatizadas*. <https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos/derecho-no-ser-objeto-de-decisiones-individuales>
- Alet, J. (2024, 4 junio). La inteligencia artificial aplicada de forma ‘eficaz’ al marketing, *Revistas Harvard Deusto*. <https://www.harvard-deusto.com/la-inteligencia-artificial-aplicada-de-forma-eficaz-al-marketing>
- Antonov, A. (2022). Gestionar la complejidad: la contribución de la UE a la gobernanza de la inteligencia artificial. *Revista CIDOB D’afers Internacionals*, 131, 41-68.
- Balaguer Callejón, F. (2022), *La constitución del algoritmo. El difícil encaje de la constitución analógica en un mundo digital*, Fundación Manuel Giménez Abad, 2º edición.
- Beard, F. K. (2017). The Ancient History of Advertising: Insights and Implications for Practitioners. *Journal Of Advertising Research*, 57 (3), 239-244.
- Bradford, A. (2021, 11 enero). *The Brussels Effect Comes for Big Tech*. Project Syndicate. Project Syndicate. <https://www.project-syndicate.org/commentary/eu-digital-services-and-markets-regulations-on-big-tech-by-anu-bradford-2020-12>
- Comisión Europea (s.f.) *Estrategia Europea de datos*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es
- Comisión Europea (s.f.). *Configurar el Futuro Digital de Europa: Ley Europea de Gobernanza de Datos*. <https://digital-strategy.ec.europa.eu/es/policies/data-governance-act>
- Comisión Europea (s.f.). *La década digital de Europa: metas digitales para 2030*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es
- Comisión Europea (s.f.). *Data Act explained*. <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>

- Comisión Europea. (2024, 3 febrero). *Preguntas y respuestas sobre la Ley de Servicios Digitales*.
https://ec.europa.eu/commission/presscorner/detail/es/QANDA_20_2348
- Comisión Europea. *Índice de Economía y Sociedad Digitales (DESI)*. (s. f.).
[Europa. https://digital-strategy.ec.europa.eu/es/policies/desi](https://digital-strategy.ec.europa.eu/es/policies/desi)
- Concellón, P. (2018). El concepto de dato personal en la Unión Europea: una pieza clave en su protección. *Revista General de Derecho Europeo / General Journal Of European Law*, 46.
https://digibuo.uniovi.es/dspace/bitstream/10651/51099/2/PilarConc_ConcDato.pdf
- Consejo de la UE (s.f.) *Inteligencia Artificial*.
<https://www.consilium.europa.eu/es/policies/artificial-intelligence/#0>
- Cordero Álvarez, C. I. (2024). El régimen de responsabilidad de las plataformas online en la DSA ante contenidos ilícitos lesivos de derechos fundamentales. En J. J. Castelló Pastor (dir.), *Análisis del reglamento (UE) de Servicios Digitales y su interrelación con otras normas de la UE*, Aranzadi, 69 a 108.
- Cotino Hueso, L. (2022). Nuevo paradigma en las garantías de los derechos fundamentales. En L. Cotino (dir.) *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*. Aranzadi, pp. 67-108.
- Cotino Hueso, L. (2024, 17 de enero). La primera sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial. *Diario LaLey 80*, sección *Ciberderecho*.
- Cuervo Sánchez, C. A. (2021). Efectos de la inteligencia artificial en las estrategias de marketing: Revisión de literatura. *Revista Internacional de Investigación en Comunicación ADResearch ESIC*, 24 (24), 26-41.
- De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal Of Constitutional Law*, 19(1), 41-70.
- Discurso Estado de la Unión 2020: https://state-of-the-union.ec.europa.eu/state-union-2020_es
- European Union External Acton (s. f.). *Por qué es importante la autonomía estratégica europea*.
https://www.eeas.europa.eu/eeas/por-qu%C3%A9-es-importante-la-autonom%C3%ADa-estrat%C3%A9gica-europea_es
- Fernández Hernández, C. (2024) La OCDE explica el contenido de su definición actualizada de los sistemas de Inteligencia Artificial, Diario La Ley de 6 de marzo de 2024.
<https://diariolaley.laleynext.es/dli/2024/03/07/la-ocde-explica-el-contenido-de-su-definicion-actualizada-de-los-sistemas-de-inteligencia-artificial>
- Fernández Villazón L. A. (2016). El nuevo Reglamento Europeo de Protección de Datos. *FORO. Revista de Ciencias Jurídicas y Sociales, Nueva Época*, 19(1), 395-411.
- Fernández, J. M. (2003). El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario. *Derecho y Salud*, 11(1), 37-46.

- García, J. S. (2014). Marketing hasta la última definición de la AMA (American Marketing Association). *Revista de la Asociación Española de Investigación de la Comunicación*, 1(2), 124-132.
- Garriga, A. (2023). Las exigencias de transparencia para los sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea en el nuevo Reglamento Europeo de Servicios Digitales. *Revista Española de la Transparencia*, (17 Extra)137-164.
- Girasa, R. (2021). *Artificial Intelligence as a Disruptive Technology: Economic Transformation and Government Regulation*. Palgrave Macmillan.
- Gobierno de España, (2024, 12 de enero) *Entra en vigor la Ley europea de Datos estableciendo nuevas normas para una economía de datos justa e innovadora*. https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/2024/Enero/Noticia-2024-01-12-Entra-en-vigor-Ley-Europea-Datos.html
- Gobierno de España. (2023, 19 abril). *Qué es la inteligencia artificial*. <https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr>
- Herrera De las Heras, R. (2022). *Aspectos legales de la inteligencia artificial: personalidad jurídica de los robots, protección de datos y responsabilidad civil*. Dykinson S.L.
- Hoffmann-Riem, W. (2019). *Big data: desafíos también para el Derecho*. Civitas.
- Huang, M. H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. *Journal of the Academy of Marketing Science*, 49, 30-50. <https://link.springer.com/article/10.1007/s11747-020-00749-9>
- Hupont, I., Fernández-Llorca, D., Baldassarri, S., & Gómez, E. (2024). Use case cards: a use case reporting framework inspired by the European AI Act. *Ethics And Information Technology*, 26(2). <https://doi.org/10.1007/s10676-024-09757-7>
- Kingsnorth, S. (2019). *Digital Marketing Strategy: An Integrated Approach to Online Marketing*. Kogan. <http://elibrary.gci.edu.np/bitstream/123456789/3127/1/Bt.bm.522Digital%20Marketing%20Strategy%20An%20Integrated%20Approach%20to%20Online%20Marketing%20by%20Simon%20Kingsnorth.pdf>
- Kumar, V., Ashraf, A. R., & Nadeem, W. (2024). AI-powered marketing: What, where, and how? *International Journal Of Information Management*, 102783. <https://doi.org/10.1016/j.ijinfomgt.2024.102783>
- L. Escajedo San Epifanio, *Tecnologías biométricas, identidad y derechos fundamentales*, Aranzadi, 2017, 84-85.
- LetsLaw. (2024, 17 mayo). *Reglamento de Servicios Digitales, ¿cuál va a ser su impacto?* <https://letslaw.es/reglamento-de-servicios-digitales-impacto/>
- Loreto, M., Y S, G. (2005). Evolución de la terminología del marketing de ciudades. En J. Gómez (Coord.), *Comunicar y enseñar a comunicar el conocimiento especializado: Homenaje a*

- Amelia de Irazazábal* (pp. 3-6). Instituto Cervantes.
<https://cvc.cervantes.es/lengua/aeter/comunicaciones/florian.htm#np2>
- Lynskey O. (2014). Deconstructing Data Protection: The ‘Added-Value’ of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly*, 63(3):569-597.
- Medina-Chicaiza, R. P., y Martínez-Ortega, A. G. (2020). Tecnologías en la inteligencia artificial para el Marketing: una revisión de la literatura. *Pro Sciences: Revista De Producción, Ciencias e Investigación*, 4 (30), 36-47.
- Meseguer, P. y López de Mántaras, R. (2017). *Inteligencia artificial*. España: Los Libros de La Catarata.
- Moreno, G./Statista Daily Data. (2019). *Infografía: A la espera de un Big Bang de datos*.
<https://es.statista.com/grafico/17734/cantidad-real-y-prevista-de-datos-generados-en-todo-el-mundo/>
- Ni Loideain, N. (2018). A Port in the Data-Sharing Storm: The GDPR and the Internet of Things. *King’s College London Law School Research Paper*, nº 2018
<https://doi.org/10.2139/ssrn.3264265>
- Nikolinakos, N. T. (2023). *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act*. Springer Nature.
- OECD, iLibrary. (s.f.). *La inteligencia artificial en la sociedad*. <https://www.oecd-ilibrary.org/sites/603ce8a2-es/index.html?itemId=/content/component/603ce8a2-es#:~:text=Las%20fases%20del%20ciclo%20de,el%20funcionamiento%20y%20el%20seguimiento>.
- Pasquali, M. (2023, 6 abril). ¿En qué países se invierte más en inteligencia artificial? *Statista Daily Data*. <https://es.statista.com/grafico/29671/paises-con-mas-inversion-privada-en-inteligencia-artificial/>
- Presno Linera, M. A. (2022), *Derechos fundamentales e Inteligencia Artificial*, Marcial Pons.
- Rincón, M. A. (2024). Aproximación a la propuesta legislativa europea sobre inteligencia artificial. *Quaderns IEE: Revista de l’Institut d’Estudis Europeus*, 3(1), 110-124.
- Sánchez, Á. A. (2020). Marco Europeo para una inteligencia artificial basada en las personas. *International Journal Of Digital Law*, 1(1), 65-77.
- Selman, H. (2017). *Marketing digital*. Ibukku.
- Stanford University (2024). *Artificial Intelligence Index Report 2024*.
https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf
- Stone, M., Aravopoulou, E., Ekinci, Y., Evans, G., Hobbs, M., Labib, A., Laughlin, P., Machtynger, J., & Machtynger, L. (2020). Artificial intelligence (AI) in strategic marketing decision-making: a research agenda. *The Bottom Line*, 33(2), 183-200.

Tajadura Tejada, J. (2021). *Los Derechos fundamentales y sus garantías*, 2ª edición, Tirant lo Blanch, p.42-43.

Unión Europea. (s. f.). *Comité Europeo de Protección de Datos (CEPD)* https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_es

7.2 Documentos Institucionales

Agencia Española de Protección de Datos (2023, septiembre). *Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo*. <https://www.aepd.es/guias/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>

Agencia Española de Protección de Datos. (2020, febrero). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*. <https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf>

Comisión Europea (2020, 19 de febrero). *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado en la excelencia y la confianza*. COM (2020) 65 final.

Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, (2019a). *Una definición de la Inteligencia Artificial: Principales capacidades y disciplinas científicas*, Oficina de Publicaciones.

Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, (2019b). *Directrices éticas para una IA fiable*, Oficina de Publicaciones. <https://data.europa.eu/doi/10.2759/14078>

Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, (2024). *El Reglamento de Servicios Digitales (Digital Services Act - DSA) explicado: medidas para proteger a los niños y los jóvenes en línea*, Oficina de Publicaciones de la Unión Europea. <https://data.europa.eu/doi/10.2759/34220>.

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Relativa a la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital Un mercado único digital conectado para todos*. Bruselas 10.5.2017, COM (2017) 228 final.

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Generar confianza en la inteligencia artificial centrada en el ser humano*, Bruselas 8.4.2019 COM (2019) 168 final.

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Inteligencia Artificial para Europa*, Bruselas 25.4.2018. COM (2018) 237 final. <https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52018DC0237>

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Brújula Digital 2030: el enfoque de Europa para el Decenio Digital*. Bruselas, 9.3.2021 COM (2021) 118 final. https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0022.02/DOC_1&format=PDF
- Consejo de Europa (2024). *Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. <https://rm.coe.int/1680afae67>
- Consejo de la Unión Europea (2016, 14 de noviembre). *Council conclusions on implementing the EU global strategy in the area of security and defence Foreign Affairs*. <https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf>
- Declaraciones comunes Parlamento Europeo Consejo Comisión Europea *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital* (2023/C 23/01) [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123\(01\)](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01))
- Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital (s.f.). *El reglamento de IA, en resumen*. https://portal.mineco.gob.es/es-es/digitalizacionIA/sandbox-IA/Documents/20220919_Resumen_detallado_Reglamento_IA.pdf
- Grupo de trabajo sobre protección de datos del artículo 29 (2018, 6 de febrero). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. <https://www.aepd.es/documento/wp251rev01-es.pdf>
- OECD (2023), *The state of implementation of the OECD AI Principles four years on*, OECD Artificial Intelligence Papers, No. 3, OECD Publishing, Paris, <https://doi.org/10.1787/835641c9-en>.
- OECD (2024). *Explanatory memorandum on the updated OECD definition of an AI system*, OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, <https://doi.org/10.1787/623da898-en>.

7.3 Seminarios de expertos/ponencias

- Filibi I. (2024, 24 de enero). *La estrategia digital europea y el proceso de elaboración del reglamento europeo de inteligencia artificial*. Seminario Iberoamericano de Expertos Hacia un marco regulador de la IA: Retos en perspectiva comparada, UPV/EHU. Bilbao, España.

7.4 Normativa

- Carta de los Derechos Fundamentales de la Unión Europea, 18 de diciembre del 2000.
- Constitución española. (BOE núm. 311, de 29 de diciembre de 1978).
- Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho. CM(2024)52-final

Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (DOUE L 281 de 23.11.2095, pp. 0031–0050).

Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. (BOE núm. 243, de 10 de octubre de 1979).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE núm. 294, de 6 de diciembre de 2018).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (DOUE L 119 de 4.5.2016, p. 1–88).

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. (DOUE L 277 de 27.10.2022, p. 1–102).

Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo de 13 de diciembre de 2023 sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (DOUE L-2023-81895 de 22.12.2023, p 1-71)

Reglamento (UE) 2024/XXX. Versión empleada: Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM (2021)0206 – C9-0146/2021 –2021/0106(COD)).

Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

7.5 Jurisprudencia

Sentencia del Tribunal Constitucional 292/2000 del 30 de noviembre. ECLI:ES:TC:2000:292

Sentencia del Tribunal Constitucional 96/1998 del 4 de mayo. ECLI:ES:TC:1998:94

Sentencia del Tribunal Constitucional 27/2020 del 26 de marzo. ECLI:ES:TC:2020:27

Sentencia del Tribunal de Justicia de la Unión Europea de 29 de enero de 2008, C-275/06, ECLI:EU:C:2008:54.

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera) de 7 de diciembre de 2023, C-634/21, ECLI:EU:C:2023:957.

Sentencia del Tribunal Supremo (sala Primera de lo Civil) 1495/2024 de 19 de marzo. ECLI:ES:TS:2024:1495.