EGUZKILORE
Número 28.
San Sebastián
2014
253-274

LA PRIVACIDAD EN EL DISEÑO Y EL DISEÑO DE LA PRIVACIDAD, TAMBIÉN DESDE EL DERECHO PENAL

Norberto J. DE LA MATA BARRANCO

Catedrático de Derecho Penal de la Universidad del País Vasco (UPV/EHU)

Desirée BARINAS UBIÑAS

Doctora en Derecho por la Universidad del País Vasco (UPV/EHU)

(A Ignacio Muñagorri, tras culminar una honrada vida universitaria)

Resumen: El desarrollo de tecnologías protectoras de la privacidad como camino para garantizar la posibilidad de anonimato es un tópico cada vez más presente en las legislaciones internacionales. Lo que en la actualidad se discute, y aquí se plantea, es la necesidad de intervención penal para promover, preventiva y anticipadamente, actuaciones que obliguen a dichas tecnologías.

Laburpena: Anonimatua bermatzeko bidean pribatutasuna babestuko duten teknologiak garatzeko aukera gero eta maizago ageri da nazioarteko legedietan. Gaur egun eztabaidatzen dena zera da, beharrezkoa ote den zigorrak ezartzea modu prebentiboan eta aurretiaz sustatzeko teknologia horiek nahitaezko bilakatuko dituzten ekintzak. Eztabaidagai hori aztertzen da hemen.

Résumé : Le développement des technologies de protection de la vie privée comme un moyen de garantir la possibilité de l'anonymat est un sujet de plus en plus présent dans les lois internationales. Ce qui est actuellement en discussion et qui se pose ici, est la nécessité d'intervention pénale pour promouvoir, d'avance et de façon préventive, des actions qui obligent ces technologies.

Summary: The development of privacy-enhancing technologies as the path to anonymity is a topic increasingly present in international laws. What is currently discussed, and here arises, is the need of criminal laws to provome, in advance and with preventive intervention, actions that compel such technologies.

Palabras clave: Privacidad en el diseño, autodeterminación informativa, autodeterminación decisional, tutela penal de la privacy, tecnologías que refuerzan la privacidad.

Hitz gakoak: Pribatutasuna diseinuan, informatzeko autodeterminazioa, erabakitzeko autodeterminazioa, pribatutasunaren babes penala, pribatutasuna sendotzen duten teknologiak.

Mots clés : Vie privée dans la conception, autodétermination informationnelle, autodétermination décisionnelle, protection pénale de la vie privée, technologies qui améliorent la protection des renseignements personnels.

Keywords: Privacy by design, informational self-determination, decisional self-determination, privacy criminal protection, privacy-enhancing technologies (PETs).

I. LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA: UN CAMBIO DE CONTEXTO Y UN CAMBIO DE VISIÓN

Durante mucho tiempo hemos sido testigos de cómo se ha ido configurando el derecho a la vida privada como garantía para la autodeterminación de la persona, dentro de una esfera propia a salvo de injerencias e intromisiones no deseadas.

Y hemos comprobado también cómo, en las últimas décadas, la "*privacy*" se ha erigido como valor a proteger también en el mundo "virtual".

Circunscrita originariamente su tutela al espacio domiciliario, al secreto de la correspondencia y al secreto profesional, extendida a "las palabras" y a la imagen en lugares "privados" y comprendiendo finalmente los "datos", como piezas de un rompecabezas capaces de revelar informaciones, tendencias e incluso realidades, muchas veces ignoradas por nosotros mismos, el boom de las nuevas tecnologías pone en solfa la cuestión de si aun con esta expansión hemos llegado a tener, y tenemos de verdad, la protección que necesitamos.

1. Valores e intereses en mutación dentro de una sociedad en permanente evolución

El impacto de las tecnologías de la información y de la comunicación en las relaciones sociales, económicas, políticas e incluso interculturales es hoy innegable. Hemos transitado ya, además, de una macroinformática reservada a algunos a una microinformática al alcance de todos y al desarrollo de una nanotecnología prácticamente invisible[1].

Pero, de un mundo en el que inicialmente nos vanagloriábamos del crecimiento continuo de la capacidad de los ordenadores y del tremendo desarrollo de las infraestructuras de comunicación pasamos a interactuar en un espacio virtual, que ya no suscita asombro alguno y sí en cambio preocupación, en el que la misma Internet se transforma, y de plataforma con sujetos pasivos receptores de información pasa a ser verdadera comunidad interactiva superada incluso a través de lo que se conoce como "ambiente inteligente"[2], que incorpora la tecnología a la vida diaria de las personas buscando "personalizar" las interacciones en el mundo tanto físico[3] como virtual[4].

---

1. Véase VAN DEN HOVEN, J., "The Tangled Web of Tiny Things: Privacy Implications of Nanoelectronics", *Nanotechnology & Society*, nº 3, 2009, pp. 147-162.

2. Así, DE HERT, P./GONZÁLEZ FUSTER, G./GUTWIRTH, S., "Legal safeguards for privacy and data protection in ambient intelligence", *Personal and Ubiquitous Computing,* vol. 13, nº 6, 2009, pp. 435-444.

3. Véanse BABBITT, R./CHANG, C./YANG, H. I./WONG, J., "Environment Objects: A Novel Approach for Modeling Privacy in Pervasive Computing", *Lecture Notes in Computer Science*, Ambient Assistive Health and Wellness Management in the Heart of the City, vol. 5597, 2009, pp. 166-173. También, las consideraciones de KOTZANIKOLAOU, P./MAGKOS, E., "Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments", *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 1, vol. 47, Security and Privacy in Mobile Information and Comunication Systems, Part 2, pp. 53-64.

4. POULLET, Y., "About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?", *Data Protection in a Profiled World*, London, 2010, pp. 3-9.

Hoy en día es común escuchar que formamos parte de la "Sociedad de la Información", que estamos en una "Era digital" en la que se ha multiplicado la capacidad de generar, tratar, transmitir y compartir información y en la que las TICs se han incorporado a la cotidianidad de la actividad humana.

Y así somos testigos, y partícipes, de un cambio trascendental en la forma en que percibimos e interactuamos en y con el mundo, insertos en una sociedad cambiante cuyos valores e intereses van mutando, a todos los niveles.

Por una parte, y en primer lugar, surge un pensamiento público, estatal, en el cual el sentido de "seguridad nacional" y la necesidad de "transparencia" parecen legitimar una vigilancia ubicua y continua de todos, justificada en los grandes "temores" modernos del crimen organizado y el terrorismo, como enemigos difusos y permanentes[5].

Y así surge una presunción de "culpabilidad" en la que se abren al exterior, informalmente y sin nuestro conocimiento y menos consentimiento, espacios, en principio, privados. Todos somos potenciales terroristas, criminales y quizás, incluso, culpables. Pero, ¿de qué? ¿en qué guerra estamos que no conocemos?

Esta vigilancia y consecuente monitorización necesariamente conlleva una clasificación de la población y la generación de parámetros de aquello que es "aceptable" y de aquello que no lo es, así como la toma de decisiones sobre los individuos en su interacción con la Administración pública que se revela peligrosa. La discriminación (cuando menos, su posibilidad) es un hecho[6]. Y la creación de una sociedad con "estándares" predefinidos, difícil de evitar. Todos somos perfilados y todos estamos ya perfilados.

Pero, quizás los Estados olvidan que su único sentido es el de garantizar el desarrollo del ser humano dentro de un contexto que permita un desarrollo socio-individual pleno de libertad y seguridad. Una seguridad bien entendida que ha de permitir hacer y ser sin temor a ser vigilado, monitoreado, catalogado y/o estigmatizado en espacios autónomos. Y, más allá de su necesidad de "control" social, el Estado debe recordar éste su rol en el que el límite de la privacidad a su actuación se presenta como consustancial a su propia esencia. Como destaca Walter Peissl, la "*discusión sobre la privacidad no es sólo sobre 'derechos'; es también sobre la filosofía de la autonomía y de la libertad y, por tanto, sobre los pilares básicos de la democracia liberal*"[7]. Y si bien explica

5. En este sentido, COLEMAN, S., "E-mail, terrorism and the right to privacy", *Ethics and Information Technology*, vol, 8, nº 1, 2006, pp. 17-27. Véanse también DÍEZ RIPOLLÉS, J. L., "De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado", *Revista electrónica de ciencia penal y criminología*, nº 7, 2005, pp. 1-36, MCADAMS, A. J., "Review: Internet Surveillance after Septembre 11: is the United States becoming GreatBritain?", *Comparative Politics*, vol. 37, nº 4, 2005, pp. 179-1098 y ORTIZ PRADILLO, J. C., "El 'Remote Forensic Software' como herramienta de investigación contra el terrorismo", *INTECO-Formación, Estudios e Informes ENAC,* nº 4, 2009, pp. 1-9.

6. POULLET, "About the E-Privacy", cit., pp. 6-7, señala dentro de los peligros que surgen como consecuencia de las TIC's el desbalance del poder entre el responsable del tratamiento y la persona concernida, la re-contextualización de la información, la "obscuridad" del funcionamiento de las TIC's, el reduccionismo y el hecho de que se borren las fronteras entre el espacio físico y privado.

7. PEISSL, W., "Information Privacy in Europe from a TA Perspective", *Data Protection in a Profiled World*, London, 2010, p. 247.

Ann Cavoukian cómo *"la historia ha demostrado que la privacidad es el primer hilo a desenredar cuando un Estado libre y democrático muta en un Estado totalitario. Mientras valoremos la libertad, debemos también valorar la privacidad […]"*[8], el riesgo no es sólo el del Estado totalitario, sino simplemente el del Estado "ubicuo" que todo lo quiere saber, que en todas partes quiere estar.

Por otra parte, en segundo lugar, asistimos asimismo a la, más que consolidación, incluso dictadura de los intereses de un mercado cuyo poder marca el ritmo de la economía, de la clase política dominante (y no dominante) y de la sociedad misma, en una espiral de consumo que obliga a prospecciones para encontrar, y muchas veces generar, posibilidades de negocio.

Aquí, la recolección y manipulación de datos, a fin de poder identificar e influir del modo más efectivo posible en consumidores (que todavía no saben que lo son) es parte del motor del negocio, favorecido por una tecnología que permite de forma fácil, económica y eficaz acceder, manipular, transferir e interconectar grandes masas de información sin límite de fronteras o de tiempo[9].

Y, así, de una publicidad anónima se pasa a una personalizada, en la que el perfil del "cliente" se va configurando con todos los datos que se van generando fruto de su (o la) interacción con el mundo físico y virtual, creándose así una "imagen" integral del individuo, de su persona, sus gustos, sus elecciones, que expone aspectos de su vida privada, de su propio ser.

Claro que el ser humano debe necesariamente interactuar con el mundo para sobrevivir. Pero, esto no implica que cada una de sus interacciones fuera de espacios restringidos pueda ser vigilada, catalogada, indexada y puesta a disposición de otros. Claro que existen actividades que se desarrollan en espacios "públicos"; pero esa apertura espacial más que limitarnos como individuos debería garantizar (si así se desea, al menos) el anonimato de una acción en un entorno en el que deberíamos (si queremos) poder perdernos en la gran "masa"[10].

Aquí surge uno de los grandes problemas que plantea la Era digital, el de la reconceptualización del espacio en el que poder estar protegido. Lo público y lo privado confluyen en un espacio social en el cual, más que la naturaleza misma del ambiente (virtual o físico) en el que la persona interactúa, juegan un rol trascendental los datos que se exponen y quedan expuestos, la forma en que son tratados y la cuestión de quién tiene acceso a ellos[11].

---

8. CAVOUKIAN, A., "Privacy by design: the definitive workshop*", Identity in the Information Society*, vol. 3, nº 2, 2010, p. 248.

9. Sobre las tendencias del mercado y las políticas de privacidad en el comercio electrónico, JOHNSON-PAGE, G. F./THATCHER, R. S., "B2C data privacy policies: current trends", *Management Decision*, vol. 39, nº 4, 2001, pp. 262-271.

10. En lo que respecta a la percepción de la protección de la privacidad en los espacios públicos, FRIEDMAN, B./HAGMAN, J./KAHN, P. H., "The Watcher and the Watched: Social Judgments about Privacy in a Public Place", *Computer Supported Cooperative Work*, Media Space 20 + Years of Mediated Life, 2009, pp. 145-176.

11. Sobre la dificultad de separar lo público y lo privado y el surgimiento del "hogar virtual", POULLET, "About the E-Privacy", cit., pp. 23-27.

Imaginemos el siguiente escenario. Una persona, en la terraza del restaurante de una plaza pública, bebe una copa, paga con su tarjeta de crédito y se marcha. Se encuentra en un lugar público, expuesto a todo el que pasa; acepta recibir un servicio, lo que todos pueden observar. ¿Tiene el propietario del restaurante derecho a conservar la huella digital dejada en el cristal de la copa, a obtener el ADN expuesto en la saliva que tuvo contacto con la copa y a relacionar todo ello con el nombre del titular de la tarjeta de crédito, la entidad bancaria emisora e incluso el número de cuenta asociado a la misma, con el tipo de bebida que pidió y con cuánto gastó? Seguramente diríamos que no. Debiéramos decir que no.

¿Por qué entonces resulta tan difícil aceptar que la huella electrónica que dejamos en la red y los datos que se revelan en transacciones puntuales no deben ser recolectados, tratados e interconectados? El mercado clama su buena voluntad y su deseo de "servir" mejor al cliente. ¿Pero es esto suficiente? ¿Es aceptable? ¿Quién ha decidido que una persona quiere recibir ofertas de productos y servicios? ¿A quién le conviene esto? ¿Justifican estos intereses del negocio una intromisión en la vida privada del individuo y una total exposición de su ser? ¿Con qué finalidad? Ni siquiera hablamos de un "interés general" a salvaguardar, sino de ese interés, que se presume anónimo, del, según se dice, "mercado".

La protección administrativa frente al tratamiento de datos personales parece estar plenamente consolidada. Las sombras sin embargo son importantes. ¿Cómo saber que se está recolectando información? ¿Cómo controlar tratamientos no declarados? ¿Y no autorizados? ¿Cómo restringir la tutela a los datos personales cuando todos acaban siéndolo, debidamente interconectados?

En tercer lugar, nos enfrentamos a una sociedad de consumo donde la nueva moda en la que se fundamentan las interacciones sociales acude al exhibicionismo y el voyerismo y se deja arrastrar por la sed irracional de "pertenecer" a una realidad construida por otros, paradójicamente, desde un sentimiento de protección por la, se dice, "impersonalidad" del espacio virtual[12]. Y, paradójicamente también, en esta realidad, en la que necesitamos ver y ser vistos, todos los que en ella actuamos nos desenvolvemos como generadores de datos y como responsables (debiéramos serlo) de los que manejamos. Se trata, en defintiva, de una interacción en la que los usuarios intercambian su privacidad por un servicio de "interconexión" social, sin ser conscientes, muchas veces, de a qué se renuncia[13].

De hecho, uno de los principales problemas a que se enfrenta esta "nueva" Sociedad de la Información es el del falso consentimiento sobre los datos que se "ceden"[14], pues muchas veces (si no siempre) hablamos de estructuras en las cuales

12. A este respecto, es interesante el artículo sobre los análisis de psicólogos relativos la tendencia de los adolescentes en la Web de LEIGHTON, P., "Uso excesivo de las redes sociales tiende a borrar el límite entre lo público y lo privado", *El Mercurio*, Chile, 25 de junio de 2011, p. A14.

13. A este respecto, DIX, A., "Built-in privacy – no panacea, but a necessary condition for effective privacy protection", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 257-265.

14. Véanse LE MÉTAYER, D./MONTELEONE, S., "Automated consent through privacy agents: Legal requirements and technical architecture", *Computer Law & Security Review*, vol. 25, nº 2, 2009, pp. 136-144 y SCHWARTZ, P. M., "Internet Privacy and the State", *Connecticut Law Review*, vol. 32, 2000, pp. 821-828.

no es negociable el nivel de exposición del ser y, así, nos encontramos ante acuerdos de "tómalo o déjalo" en los que esta última opción implica la autoexclusión. Piénsese en la interacción con páginas web que exigen el registro de los participantes, los acuerdos de adhesión con los prestadores de redes sociales y otros servicios de la Web 2 o incluso la exigencia de datos personales (e-mail, etc.) para poder acceder a un servicio cualquiera (no virtual, sino real, en el ámbito del ocio personal, la utilización de servicios bancarios, etc., pero vehiculizado en un "alta" que acude, aquí sí, a la obtención de datos a digitalizar). ¿Se puede hablar realmente de un poder de decisión, de un acuerdo en posición de igualdad?[15].

Y, en relación con todo ello, en cuarto lugar, surge, como casi siempre, un Derecho penal estatal (pero en todos los Estados), más simbólico que nunca, deslumbrado aparentemente por la "ciberrealidad", que propone, porque así lo proponen Decisiones internacionales, la protección (penal) de la integridad y la confidencialidad de sistemas y datos. Prescindiendo, sin embargo, a menudo, del hecho de que al fin y al cabo esas pulsaciones que flotan en el aire, que circulan por las redes y que se transmiten en el ciberespacio son importantes por lo que representan. Así, se penalizará en muchos ordenamientos el acceso ilícito a un sistema, pero sin tener en cuenta el acceso, tremendo, "desconocido" (y parece que lícito) porque no es "directo". Se aludirá a la sensibilidad o personalidad de determinados datos, pero sin tener en cuenta que casi todos acaban siéndolo con una tecnología que permite la interconexión de información de forma masiva. Se permitirá la perfilación de caracteres, la asignación de roles, la ubicación de personas en compartimentos estancos, pero sin que el ubicado sepa por qué y de modo, parece, lícito, porque simplemente se han utilizado las huellas que "voluntariamente" vamos dejando en el espacio virtual.

¿Cómo hacer entender que no se trata sólo del acceso ilícito a la información o del control de ésta, sino del derecho (siempre) a ser "dejado en paz"? ¿Cómo hacer comprender que no se trata de garantizar un uso o un tratamiento "legítimo" de los datos sino de evitar que los datos puedan generarse y, en su caso, incluso, de garantizar la desconexión sin que eso signifique renunciar a "ser" en la era digital? ¿Cómo insistir en la importancia del carácter decisional, también, del derecho a la privacidad? ¿Cómo en la necesidad de la importancia de tutelar la autodeterminación no sólo informativa del individuo sino la que concede la libertad de decidir quién soy, qué quiero y cómo me interesa interactuar en el espacio a salvo de predicciones, de definiciones, de clasificaciones obtenidas del intercambio de datos que he ido dejando en el camino?

La paz a la que aludieron Brandeis y Warren implica disponer de un espacio, más allá de la distinción entre lo físico y lo virtual, que pertenece al individuo como fundamento de su misma existencia y que no se entiende sin la posibilidad de poder evitar ser observado, monitoreado, clasificado, estandarizado, transformado en un algoritmo computacional, para que nuestras opciones (en todos los ámbitos de la vida) no las marquen otros, no aparezcan predeterminadas por decisiones triviales que hemos ido tomando a lo largo de la vida pero que hemos de tener derecho a poder cambiar.

---

15. En este sentido POULLET, "About the E-Privacy", cit., pp. 3-30.

En definitiva, la utilización de las tecnologías que caracteriza a la Sociedad de la Información va de la mano de las dudas que suscita la dependencia de ellas y su ubicuidad[16]. En sí, son neutras, es cierto; no estamos sino ante algoritmos, combinaciones, ceros y unos. Pero su uso no lo es[17]. Y no lo es porque la lógica en base a la que se han desarrollado viabiliza una trazabilidad y monitoreo continuo, invisible y general[18].

Martin Cooper, a quien se atribuye la invención del teléfono móvil, en el discurso inaugural de la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Madrid en 2009 loaba las innumerables ventajas que traerán las nuevas tecnologías todavía por venir poniendo como ejemplo la implantación de nano *tags* que permitan monitorear los signos vitales y el comportamiento de los órganos de las personas y avisar a emergencias en el caso de anomalías o incluso suministrar descargas que regularicen el funcionamiento de los mismos. Sí. Pero, ¿quién va a conocer esas anomalías, quien va a monitorear mis signos vitales y, sobre todo, qué rastros van a ir generando esos datos que un fin tan loable y otro y otro y otro más van a exigir?

Pues bien, si como decía Lessig que "*el código es la ley*"[19], será la ley la que haya de moldear el código.

2. Un cambio de contexto y de paradigma en la protección, también penal, de la vida privada

No es posible decidir qué hacer o cómo proceder en este escenario sin comprender el contexto en el que actúa el Derecho penal y, en concreto, su tutela de la vida privada.

¿Estamos comprendiendo realmente el problema? ¿Estamos acertando a la hora de seleccionar las conductas a sancionar para prevenir la lesión del interés que queremos garantizar?

El Derecho penal, difícil que sea de otro modo, adquiere casi siempre un papel reactivo[20], siguiendo los cambios sociales y tratando de prever amenazas futuras a intereses consagrados. Por ello mismo, para cuando se cuenta con instrumentos (suponiendo además que se quiera contar con ellos, venciendo la resistencia de impor-

16. Sobre la ubicuidad informática y el respeto de la vida privada, LANGHEINRICH, M., "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems", *Lecture Notes in Computer Science,* Ubicomp, vol. 2201, 2001, pp. 273-291.

17. Entre otros, BURNIK, J./PIRC MUSAR, N., "The Dangers of Electronic Traces: Data Protection Challenges Presented by New Information Communication Technologies", *Lecture Notes in Computer Science, Ethics and Policy of Biometrics*, vol. 6005, 2010, pp. 7-13.

18. A esto se agrega el aumento en la capacidad de percibir y sentir el ambiente (incluyendo aspectos emocionales de las personas) –lo que implica una ampliación del espectro controlado por las tecnologías y de los datos almacenados e interconectados– y en el desarrollo de la memoria digital y de su capacidad de análisis: a este respecto, LANGHEINRICH, "Privacy by Design", cit., pp. 273 ss.

19. LESSIG, L., *Code: and other laws of Cyberspace*, version 2.0 Basic Books, New York, 2006, pp. 1 ss.

20. En este sentido, y en este contexto, DIX, "Built-in privacy", cit., pp. 257-258.

tantes poderes fácticos) eficaces, conscientes de los nuevos peligros, éstos ya no son tales sino menoscabos concretos a esos intereses que, consagrados, creemos salvaguardados. La cuestión es no reaccionar excesivamente tarde.

El legislador ya ha comprendido hace tiempo que más allá del soporte o el ámbito físico que puedan representar expresiones de lo que hasta ahora era la vida privada existen determinadas informaciones que merecen tutela penal. Esto ya supuso el pasado siglo un cambio de paradigma: aceptándose que el espacio o soporte que contextualiza una comunicación o la expresión del ser de una persona no es lo que define su carácter privado o no, sino la vocación con que se externalizaron; y extendiendo la protección del individuo a "cualquier" espacio "privado" (esto es, no público).

Pero, vislumbrando que las personas generan informaciones, con diferentes formas, que siempre pueden ser captadas, registradas, transmitidas y difundidas, la tutela del derecho a la vida privada ha ido reforzando sus aspectos informacional y decisional desde un segundo cambio de paradigma atento a la masificación en el tratamiento de datos personales y a la necesidad de legitimarlo y atento al hecho de que no sólo hay que temer al propio Estado (primer gran enemigo de la privacidad), sino al resto de nosotros, parte de un gran-único mercado en que todo está a la venta. Así, las leyes de protección de datos han ido garantizando paulatinamente, es cierto, una recolección y tratamiento de información respetuosa con la privacidad, como hasta ahora se venía entendiendo.

Y, sin embargo, ha de insisitrse en que ello ha de hacerse en relación a todo tipo de información (no restringida a datos personales[21]) en cuanto cualquier dato, incluso trivial, interconectado, ensamblado y analizado permite la creación de perfiles integrales y la toma de decisiones fundamentadas en predicciones[22], ajenas a nosotros, que afectan sin duda al concepto amplio de vida privada que creemos ha de defenderse.

Más aún, es necesario comprender que el peligro para la privacidad, está no tanto -al menos, no sólo– en la naturaleza de la información protegida, sino en la generación innecesaria de la misma (además de, por supuesto, en su recolección, tratamiento y uso).

No se trata de que los datos sean "legítimamente" recolectados, tratados, usados. Se trata de cuestionar si realmente tienen que generarse (y recolectarse, tratarse y usarse). Ésta es la clave y la gran laguna de nuestras legislaciones; y es fundamental que seamos capaces de entenderlo.

Se habla en la actualidad de los delitos informáticos, de los ciberdelitos, de los delitos de alta tecnología. Se incorporan con mayor o menor acierto a las legislaciones penales internas. Se acierta a ver la importancia de la protección de infraestructuras vitales críticas; de los sistemas de información en sí mismos considerados. Se alude incluso a la "seguridad informática" como posible interés a tutelar. Se va

---

21. Por eso, en la normativa internacional acaba optándose por aludir a la protección de datos de tráfico y localización (y no solo personales). Así, por ejemplo, ya en la Directiva 2002/58/CE, en el sector de las comunicaciones electrónicas. Véase POULLET, "About the E-Privacy", cit., pp. 9-18.

22. Véanse SCHWARTZ, P. M., "Privacy, Ethics, and Analytics", *IEEE Security & Privacy*, mayo/junio 2011, pp. 66-69 y POULLET, "About the E-Privacy", cit., pp. 3 ss.

distinguiendo cada vez con mayor acierto entre delitos de contenido (que se van acomodando a los nuevos tiempos) y delitos contra sistemas y datos. Pero no se puede perder de vista la importancia de seguir garantizando lo básico. Claro que el peligro de una quiebra del sistema a gran escala está latente. Pero, sigue siendo necesario entender las amenazas a los bienes más tradicionales. Entender que se está perdiendo de vista que son comportamientos "en principio" lícitos (que parten de consentimiendos viciados, forzados, implícitos) los que van mermando la idea de privacidad. Entender que estamos expuestos, abiertos a todos, sin muchas veces saberlo (mucho menos quererlo). Por eso, ¿qué más da que sancionemos los accesos no consentidos si constantemente se está utilizando información que no desearíamos que se utilizase y que no sabemos se utiliza?

¿Qué justifica el desarrollo de una infraestructura tecnológica intrusiva y ubicua? ¿Qué justifica la recolección de información, su tratamiento y su difusión? ¿Qué justifica que la moneda de cambio en el mundo virtual sean nuestros datos, nuestra privacidad? ¿Es siempre realmente necesaria la interconexión de la información y la creación de perfiles?

3. En búsqueda de una respuesta jurídica acertada frente a una realidad cambiante

Dentro del contexto digital la infraestructura tecnológica que lo soporta es justamente la que marca la forma en que interactuamos con ella; en la medida que a través de ella se definirá qué es capaz de hacer cada dispositivo, programa o herramienta tecnológica y, más importante aún, cómo lo hace, será básico definir y regular las fuerzas que la motorizan y los intereses que han de tomarse en cuenta para su diseño.

La respuesta del legislador ha sido hasta ahora la de responder a los riesgos o amenazas que se asocian al desarrollo exponencial de las nuevas tecnologías, de modo tardío, condicionado e insuficiente. Tardío porque los daños a bienes jurídicos importantes ya se han producido y seguirán produciéndose en cuando las propias tecnologías albergan en el seno de su configuración la capacidad de atentar contra la privacidad. Condicionado porque reacciona sólo antes casos puntuales. Insuficiente porque las soluciones encontradas no parten de un análisis real de la raíz del problema, limitándose a corregir déficits concretos. Y siempre focalizado a responder a las consecuencias no a las causas de los problemas que se van poniendo de relieve.

Una infraestructura tecnológica, cuyos avances se financian y definen, casi siempre (siempre, en realidad) por el mercado o por el Estado (en especial, por su aparato militar), que difícilmente tendrá en cuenta los intereses de los ciudadanos, genera dudas evidentes.

Siendo así, el legislador, incluido claro el penal, debe: primero, entender que el desarrollo tecnológico no ha hecho sino comenzar, por lo que el concepto de neutralidad tecnológica debe ser tenido en cuenta a todos los niveles de tutela jurídica, lo que implica decidir qué es lo que realmente se quiere proteger, más allá de lo envolvente que puedan ser las ideas de ciberespacio, mundo virtual o alta tecnología y la enumeración de concretas conductas a sancionar con terminologías que seguramente pronto quedarán obsoletas; segundo, obligar a un desarrollo de las tecnologías de la información y comunicación que tome en cuenta la tutela de la vida privada, sobre

todo, como una condicionante necesaria de su diseño, y en las que retorne a los usuarios el verdadero control sobre su información e interacción con ella en el mundo virtual; tercero, evitar que nadie pueda ser involuntariamente perfilado, clasificado, codificado y, con ello, discriminado o excluido, lo que sólo es posible desde la reafirmación del derecho a que no se generen datos que no se quieran generar[23], a la desconexión, al olvido y, en el más amplio sentido de la expresión, a ser "dejado en paz". Sólo así se garantiza realmente (física y virtualmente) la dimensión interior del ser humano que le permite desarrollarse libremente sin injerencias no ya no autorizadas o arbitrarias sino simplemente innecesarias (para él).

Es la idea, como se decía, de alguna decisión internacional, de la que es exponente, por ejemplo, la Directiva 2002/58/CE, sobre privacidad y comunicaciones electrónicas, cuando afirma en su art. 14.3: "*Cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales*". Más garantista habría sido sustituir la expresión "cuando proceda", por la de "por defecto" o, simplemente, por la de "siempre"[24]. Pero, en todo caso, qué diferencia con la afirmación de la Directiva 95/46/CE que aludía a la seguridad del tratamiento de los datos según el "estado de la técnica".

Aquí es en todo caso donde debe evolucionar el Derecho penal, incorporando la sanción no sólo de "accesos ilícitos", "abusos de equipos e instrumentos técnicos", etc., como se requiere desde instancias internacionales, sino planteándose la punición de la no incorporación de parámetros de privacidad por defecto dentro de la configuración y diseño de las tecnologías[25]. La *privacy by design* se plantea como una necesidad en este contexto. Destacada en el plano internacional como uno de los tópicos relevantes abordados en las Conferencias Internacionales de Autoridades de Protección de Datos y Privacidad celebradas en 2009 y 2010[26], presente en el Programa de 2011[27] y ya referenciado en 1995 en el informe de Ann Cavoukian y John Borking "*Privacy-enhancing technologies: the path to anonymity*"[28] es una expresión que también en el ámbito penal merece toda nuestra atención.

---

23. Señala SCHAAR, P., "Privacy by Design", *Identity in the Information Society*, vol. 3, nº 2, 2010, p. 273, que hay que tener en cuenta en el diseño de las TICs la minimización de la data, la facilidad de control sobre ella, la transparencia en el "cómo" se maneja, la calidad, confidencialidad y posibilidad de segregación de la misma.

24. Coincidimos con POULLET, "About the E-Privacy", cit., pp. 20-21, cuando destaca que si bien la Unión Europea tiende a apoyar en sus recomendaciones el desarrollo de las llamadas PET's o *Privacy-Enhancing Technologies*, es criticable que aún no exija la obligación de implementar parámetros protectores de la privacidad. A esto hay que agregar que limitar la vía de protección del derecho a la vida privada a unas "determinadas" tecnologías nos parece no sólo arriesgado sino insuficiente. Dentro de una realidad tecnológica en constante evolución es posible que se desarrollen mecanismos mucho más efectivos para su protección.

25. Véase SCHAAR, "Privacy by Design", cit., 267-274.

26. Respectivamente, en http://www.privacyconference2009.org y http://www.justice.gov.il/PrivacyGenerations/program.htm.

27. En http://www.privacyconference2011.org/includes/Draft_Programme_Espanol.pdf.

28. Véase HUSTINX, P., "Privacy by design: delivering the promises", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 253-255. Asimismo, INFORMATION AND PRIVACY COMMISSIONER/REGISTRATIERKAMER, *Privacy-Enhancing Technologies: The Path to Anonymity*, vol. I y II, 1995, (en http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf).

II. LA TECNOLOGÍA COMO ALIADA DEL DERECHO Y EL DERECHO COMO ALIADO DE LA TECNOLOGÍA: PRIVACIDAD EN EL DISEÑO ("PRIVACY BY DESIGN")

La tecnología plantea problemas. Pero ella misma puede aportar soluciones. El primer cambio de visión necesario para lograr una tutela de intereses no cuestionados (o que no debieran serlo) es el de que las Tecnologías de la Información y la Comunicación no necesariamente tienen que configurarse partiendo de una infraestructura de vigilancia y trazabilidad[29]. A partir de ahí necesitamos respuestas tecnológicas apoyadas legalmente. La idea de la *privacy by design* (privacidad en el diseño), desarrollada en Canadá[30] y Holanda[31], va en esta dirección.

Sin embargo, incorporar en el diseño tecnológico la idea de privacidad, construyendo entornos amigables y garantes de este derecho, no es sino un primer paso al que ha de seguir la toma de conciencia de las personas de cómo protegerse de las consecuencias de sus elecciones y de la puesta a disposición –de quien quiera o pueda utilizarlos– de sus datos, así como el conocer las herramientas con que cuentan para ello, creando verdaderamente un entorno donde la elección de parámetros protectores de la vida privada no conduzcan a una especie de auto-exclusión.

No se trata sólo de "navegar" protegidos, sino de navegar "seguros"; seguros de nuestras elecciones, seguros de que se respetarán nuestros derechos, de que no se violará nuestra privacidad, de nuestra facultad de autodeterminación personal y del respeto de ése, nuestro espacio privado, más allá de su carácter corporal o incorporal. Esta "seguridad" sólo puede construirse a través de la concienciación de las personas y del desarrollo de ambientes que viabilicen un verdadero diálogo, donde libertades y derechos no negociables no sean moneda de cambio de los servicios ofrecidos. Y esto sólo será posible de la mano de la legislación. La tecnología como aliada del Derecho y el Derecho como aliado de la tecnología, se dirá[32].

La incorporación de una visión protectora de la privacidad como parámetro necesario en el desarrollo de las nuevas herramientas y dispositivos tecnológicos es una perspectiva que ha sido tímidamente incorporada en diferentes regulaciones[33], aunque más como reacción ante las amenazas de tecnologías ya desarrolladas.

---

29. Esto implica que debe incorporarse en la conceptualización misma del sistema y como requisito indispensable la protección de la privacidad. En este contexto, PEARSON, S./YUN, S., "Context-Aware Privacy Design Pattern Selection", *Lecture Notes in Computer Science*, Trust, Privacy and Security in Digital Business, vol. 6264, 2010, pp. 69-80. También, entre otros muchos, CHARLESWORTH, A./PEARSON, S., "Accountability as a Way Forward for Privacy Protection in the Cloud", *Lecture Notes in Computer Science*, Cloud Computing, vol. 5931, 2009, pp. 131-144 y DEY, A. K./HONG, J. I./LANDAY, J. A./LEDERER, S., "Personal privacy through understanding and action: five pitfalls for designers", *Personal and Ubiquitous Computing*, vol. 8, nº 6, 2004, pp. 440-454.

30. El concepto se atribuye a CAVOUKIAN, A., *Privacy by design…take the challenge*, Whasington D. C., 1997, pp. 3-7, Comisionada de Información y Privacidad en Canadá.

31. Véase HUSTINX, "Privacy by design", cit., p. 253.

32. Véase SCHWARTZ, P. M., "Internet Privacy and the State", cit., pp. 815 ss., quien clama por la necesidad de la intervención estatal a fin de configurar adecuadamente el mercado y las normas protectoras de la *privacy*.

33. A este respecto DIX, "Built-in privacy", cit., p. 257.

Y, sin embargo, la única forma real y efectiva de garantizar una verdadera protección del derecho a la vida privada es comprender que es hora de repensar las tecnologías y de tomar en cuenta desde el diseño mismo que precede a su materialización la necesidad de considerar ciertos parámetros no negociables[34].

Hasta ahora ha primado, incluso en el desarrollo mismo de muchas legislaciones, el sentimiento de que la privacidad es más bien un "freno" –o un derecho que es posible relegar a un segundo plano y, por supuesto, renunciable– frente a las ideas de rentabilidad del mercado (en lo privado)[35] y de seguridad (en lo público)[36]. Así, pareciera, por una parte, que las personas existen para consumir, porque lo exige un "mercado anónimo", en tanto, por otra, se desarrolla una sociedad del temor, aparentemente siempre en guerra y con enemigos difusos, pareciendo incluso que lo somos todos nosotros cuando nos resistimos a participar de medidas "a favor" de "¿nuestra? seguridad".

Ahora bien, el mercado existe para satisfacer –de verdad– las necesidades de las personas; el Estado, para garantizar la dignidad y el libre desarrollo de los seres humanos. Y la relación entre desarrollo del mercado, seguridad y privacidad debería ser la de ganar, ganar, ganar y vuelta a ganar. Pero, todos. Ello exige, en nuestra opinión, la incorporación en el desarrollo tecnológico de una nueva filosofía en que la privacidad sea un elemento nuclear a tomar en cuenta dentro del diseño y arquitectura de las tecnologías, herramientas, programas, dispositivos, sistemas y demás avances que acompañen el desarrollo humano y científico.

1. La filosofía de la privacidad en el diseño (o el diseño de la privacidad)

Ann Cavoukian define la *privacy by design* como "*la filosofía y el enfoque de incorporar la privacidad en el diseño de las diferentes tecnologías*"[37]. Esta autora señala que si bien ello podría conseguirse a través de la implementación de las "*Fair Information Practices"* en la arquitectura de las mismas, deben tomarse en cuenta no sólo aspectos tecnológicos, sino las prácticas del negocio y el diseño físico así como la propia infraestructura de la Red[38]. La privacidad es algo a "construir" en la estructura misma de la tecnología y en su aplicación.

Esto es importante en cuanto no se trata sólo de contar con sistemas o programas que contengan algoritmos protectores de la privacidad, sino también de tener a disposición *hardwares*, equipos e infraestructuras que puedan soportarlos, salvaguardando ellos mismos, en su construcción, este derecho, así como personas capaces de gestionar estas herramientas e incluso un espacio físico adecuado para

34. En este sentido, LE MÉTAYER, D., "Privacy by Design: A Matter of Choice", *Data Protection in a Profiled World,* Part 6, 2010, pp. 323-334.

35. Así, CAVOUKIAN, "Privacy by design", cit.

36. Sobre los conflictos entre seguridad en la Web y privacidad, JENSEN, C. D./SEIGNEUR, J. M., "Trading Privacy for Trust", *Lecture Notes in Computer Science*, Trust Management, vol. 2995, 2004, pp. 93-107.

37. CAVOUKIAN. *Privacy by design,* cit., p. 3.

38. CAVOUKIAN, "Privacy by design", cit., pp. 247 ss.

su incorporación. Se destacan entonces dos pilares en este modelo: por una parte, la construcción de una tecnología protectora de la privacidad (tanto en *software* como en *hardware* como en las infraestructuras que soporten ambos); por otra, la creación y aplicación de parámetros protectores de la privacidad que garanticen su respeto en todo el ciclo de vida de las informaciones que puedan –porque tengan que– generarse y en todos los "estados" de la implementación de la tecnología (es decir la puesta en práctica efectiva de esta protección con una visión protectora de la privacidad).

Ann Cavoukian señala también que la protección de la privacidad no debe verse como una "carga", sino como algo fundamental para salvaguardar no ya la democracia, sino un mercado mismo que se fundamenta en la confianza que se deposite en él. Enfatiza así la necesidad de erradicar esa visión de "*zero-sum*", en la cual hay que elegir entre la protección de uno u otro interés (mercado o privacidad) y partir de un paradigma "*positive-sum*" en el que todos pueden verse beneficiados sin importar las decisiones o elecciones tomadas[39].

Pero es mucho más que esto. La tendencia en el desarrollo de las tecnologías ha sido la de apostar por la pérdida de privacidad frente a otros intereses. Algo inadmisible. Son las propias tecnologías las que deben ser capaces de garantizar los derechos a los que parecen oponerse, derechos no negociables que han de conciliarse con otros pero como sumandos. La privacidad, en este sentido, no puede entrar en la ecuación como elemento desechable.

La autora canadiense destaca que la implementación de esta filosofía conlleva siete principios fundamentales: 1º que se asuma un enfoque proactivo no reactivo, preventivo no correctivo; 2º que los parámetros protectores de la privacidad se establezcan "por defecto"; 3º que la privacidad se encuentre integrada en el diseño; 4º que exista una funcionalidad total, asumiendo una visión "*positive-sum*" de la privacidad; 5º que la protección de la privacidad esté presente en todo el ciclo de vida de la información; 6º que las prácticas implementadas sean visibles y transparentes; 7º que se respete la privacidad de los usuarios[40].

Todo ello, correctamente desarrollado, debería conllevar, sin duda, la reducción de la recolección, utilización, retención y transmisión innecesarias de datos personales (en cuanto relativos a las personas, no en cuanto de índole personal-sensible) por los sistemas, al mismo tiempo que el fortalecimiento de la seguridad de la información y el empoderamiento a los individuos a fin de que ejerzan un verdadero control sobre sus propios datos[41].

Si bien es cierto que este discurso resulta poderoso y atractivo, no es menos cierto que para hacerlo realidad no bastará la transparencia de las prácticas de las empresas. Los más de quince años que han pasado desde que por primera vez surgió este nuevo paradigma de "la privacidad en el diseño" así lo han demostrado. Hará falta mucho más que la buena voluntad de algunos y está llamado el Estado, en cuanto legislador, a devolver un equilibrio hoy perdido a fin de que la suma, frente a

39. CAVOUKIAN, *Privacy by design,* cit., pp. 51-55.

40. CAVOUKIAN, "Privacy by design", cit., pp. 249-250.

41. Véase CAVOUKIAN, *Privacy by design*, cit., pp. 17 y 24.

intereses y elecciones políticas de gran peso, no se convierta en una resta en detrimento del derecho a la vida privada.

La protección de la privacidad no es negociable y no se trata sólo de crear parámetros por defecto que salvaguarden el derecho a la vida privada, que puedan ser "modificados" por los usuarios, sino la incorporación de forma integral y no mutable de determinados parámetros mínimos protectores de ella, en cuanto muchos de estos usuarios no cuentan con los conocimientos técnicos adecuados para intentar protegerse[42] y/o desconocen los riesgos de la desprotección.

Indudablemente los aspectos que destaca Cavoukian son fundamentales para un correcto desarrollo de una nueva generación de tecnologías por venir que incorpore dentro de los intereses a considerar en su diseño la protección de la privacidad en todas las etapas de su implementación[43]; para que todos salgan ganando; se trata, si se quiere, de alcanzar, en la Red inteligente, una "privacidad inteligente"[44].

Actualmente nos encontramos con tecnologías que deliberadamente prescinden de parámetros protectores de la privacidad, tecnologías que ni siquiera se plantean su impacto en ella, tecnologías que no la garantizan porque están mal diseñadas[45]. Frente a ello, hay que moldear la mentalidad de quienes están implicados en su desarrollo, analizar el impacto de cada herramienta en la privacidad, incorporar formas de auditar y corregir el comportamiento de los sistemas respecto de la configuración de sus parámetros, buscar el modo de hacerlos flexibles.

Daniel Le Métayer acertadamente señala que la elección a la hora de implementar esta filosofía es, ante todo, política; política por depender de una decisión colectiva, aunque no necesariamente concertada o democrática, llevada a cabo por los actores que tienen más peso: la sociedad (los individuos), la ley (el legislador), la tecnología (los científicos) y el mercado (la industria). Y claro, así, los individuos tienen realmemnte pocas posibilidades de influir en la construcción de diseños de privacidad, quedándoles sólo la opción de renunciar a los servicios que se les ofrecen o aceptar recortes en ella[46].

Más aún, es cierto que se han desarrollado tecnologías protectoras de la privacidad, pero el conocimiento de su existencia y su uso no son del todo accesibles a "no expertos"; por ello, el concepto de la privacidad en el diseño debe exigir ir más allá. De lo que se trata no es ya de disponibilidad. No se trata de que determinadas tecnologías estén disponibles sino de que determinados parámetros protectores de la privacidad estén integrados, siempre, en esas tecnologías de modo real.

---

42. SCHAAR, P., "Privacy by Design", cit., pp. 267 ss.

43. Véase SMITH, J./PROSCH, M, "Extending the value chain to incorporate privacy by design principles", *Identitiy in the Information Society*, vol. 3, nº 2, 2010, pp. 295-318.

44. Así, CAVOUKIAN, A./POLONETSKY, J./WOLF, C., "SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 275-294.

45. Véase LE MÉTAYER, "Privacy by Design", cit., pp. 326-327.

46. *Ibídem,* pp. 328-329.

2. Tecnologías desarrolladas para proteger la privacidad

El primer concepto con el que se relaciona la expresión "*privacy by design*" es el de las *PET's* (*Privacy-Enhancing Technologies*).

Las *PETs* se definen en el Libro Blanco sobre las tecnologías orientadas a reforzar la privacidad como "*el nombre común de una amplia gama de diferentes tecnologías para proteger los datos personales sensibles dentro de los sistemas de información*"[47]. Kenny y Borking dirán que estas tecnologías son las que hacen referencia a "*sistemas coherentes de tecnologías de la información y de la comunicación que fortalecen la protección de la vida privada de un individuo en un sistema de información mediante la prevención del procesamiento innecesario o ilegal de los datos personales u ofreciendo herramientas y controles a fin de mejorar el control de los individuos sobre su información personal"*[48]. Ambas insatisfactorias, en parte, en cuanto limitan la información a tener en cuenta a la de los datos personales (salvo en base a un concepto extensivo de éste). La primera incluso alude a la expresión "sensibles". La segunda describe una disyuntiva y, sin embargo, la privacidad ha de garantizarse tanto desde la reducción al mínimo de la recolección y tratamiento de datos como desde el empoderamiento de las personas sobre los mismos.

Las tecnologías orientadas a reforzar la privacidad (*PETs*) están normalmente asociadas a técnicas que permiten a los usuarios de sistemas de comunicación electrónica impedir que sus comportamientos y actividades sean trazados o se les identifique a través de éstos[49]. Esto conlleva que cuando se alude a ellas se piense en tecnologías que tienden a garantizar el anonimato de quien recibe y envía, a ocultar las comunicaciones en sí mismas y a impedir que se relacionen diversos eventos[50].

Se destacan también como tecnologías transformadoras, entre otras, la encriptación biométrica, el "*clipped tag"* para los *RFID* (identificación por radiofrecuencia) –que permite desactivarlos-, la encriptación de las imágenes, la protección de la imagen corporal que sólo "esboza" el cuerpo humano[51], lo que permite comprender la importancia de la expansión de su aplicación también al mundo físico.

Algunos autores identifican las *PETs* con tecnologías que se focalizan en la reducción de los datos; otros las identifican con las que dan "poder" al usuario sobre su información.

---

47. KOORN RE, R. (Editor), *Privacy-Enhancing Technologies, White Paper for Decision-Makers*, Ministry of the Interior and Kingdom Relations, Netherlands, 2004.

48. KENNY, S./NORKING, J., *The value of privacy engineering*, citado por CAVOUKIAN, *Privacy by design,* cit., p. 24.

49. Para más detalle, INFORMATION AND PRIVACY COMMISSIONER/ REGISTRATIERKAMER, *Privacy-Enhancing Technologies,* cit.

50. Véase FEDERRATH, H., "Privacy Enhanced Technologies: Methods - Markets - Misuse", *Lecture Notes in Computer Science*, Trust, Privacy, and Security in Digital Business, vol. 3592, 2005, pp. 1-9.

51. Véase CAVOUKIAN, *Privacy by design*, cit., pp. 27-35.

Se clasificarán las mismas en tecnologías de control, de segregación de datos, de consecución del anonimato y de administración de la privacidad[52].

Habrá autores, en fin, que agregarán a estas tecnologías, distinguiéndolas de las *PETs*, las que tienen activadas las opciones más protectoras de la privacidad (*privacy by default*), los metadatos en el intercambio de información, las tecnologías que previenen la transmisión no autorizada de datos (*data loss prevention*), englobando todas dentro de esas tecnologías que responden al concepto de una *privacy by design*[53].

Especialmente completo es el estudio de Dawn N. Jutla, que recoge distintas clasificaciones destacando la que distingue entre las teccnologías que garantizan la privacidad de las comunicaciones, el anonimato, los controles personales, el control sobre las interferencias o las salvaguardias corporativas. Ella, fijándose en las diferentes fases del comportamiento de los usuarios, diferenciará las tecnologías que permiten tomar conocimiento de los asuntos y derechos relacionados con la privacidad, las que permiten actuar para proteger este derecho, las que permiten detectar violaciones y las que permiten resolver conflictos relacionados con el mismo, buscando abarcar de modo completo el "ciclo de vida de la privacidad". Resalta a este respecto la denominada *P3P* o *Privacy Plataform Preferences,* cuya configuración consiste en la incorporación de una serie de opciones de privacidad que reflejan diversos niveles de protección a través de los cuales pueden definirse qué datos serán recolectados, con quién se compartirán, por cuánto tiempo se conservarán y con qué propósito[54].

La cuestión es que todo esto parte de una relación entre partes en situación de igualdad. Pero, no es así. No lo es porque el peso de la configuración de un usuario no es similar al de los demás sujetos con los que interactúa; el nivel de conocimiento y conciencia sobre las implicaciones de sus elecciones sobre su privacidad no suele ser el adecuado; las elecciones que toma suelen conducir a decisiones discriminatorias y excluyentes; y no se actúa en un ambiente transparente en que estén asegurados e integrados estándares mínimos protectores de la privacidad no negociables.

Así, en esta conceptualización acerca de la incorporación en el diseño de la privacidad cabe obervar con preocupación la tendencia a fundamentar esa "adecuada" protección tecnológica desde el prisma de la "auto-regulación" y la "negociación". Sin embargo, un sistema puede ser transparente y vulnerar con creces la privacidad de usuarios impotentes o ya afectados. Lo imporante sigue la cuestión de cuándo y en qué medida es necesario generar, recolectar y tratar la información de los sujetos que acuden a la Red. ¿Qué gana una persona cuando se le atribuye aparentemente un control sobre datos que ya circulan por la Red y cuya ingente cantidad impide una real y efectiva administración de los mismos? ¿Qué gana el usuario si un sistema parte

---

52. Veáse KÖFFEL, C./WÄSTLUND, E./WOLKERSTORFER, P., "PET-USES: Privacy-Enhancing Technology - Users' Self-Estimation Scale", *IFIP Advances in Information and Communication Technology*, vol. 320, Privacy and Identity Management for Life, 2010, pp. 266-274.

53. Véase MIRALLES, R., "Privacy by design: la privacidad en el diseño", *INTECO-Formación, Estudios e Informes ENAC*, nº 4, 2009, pp. 10-14.

54. JUTLA, D. N., "Layering privacy on operating systems, social networks, and other platforms by design", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 319-341.

de parámetros protectores de la privacidad establecidos por defecto pero que debe ir desmontando a fin de poder acceder de forma fácil y eficiente a los servicios ofertados en la Web? Téngase en cuenta, por ejemplo, la imposibilidad práctica de desactivar determinadas cookies para poder acceder a ciertos sitios o la necesidad de desactivar determinadas alarmas de seguridad, recurrentes pero innecesarias, para poder navegar con cierta libertad[55]. Y la alternativa no puede ser la de "eres libre para decidir lo que quieras, pero, según lo que decidas, te quedas fuera".

Peter Schaar señala que en el diseño de un sistema de procesamiento de datos, hay que minimizar la datos recolectados y tratados a lo estrictamente necesario, otorgar un control real sobre la información relacionada con una persona a ésta, hacer transparente el funcionamiento del sistema, salvaguardar la confidencialidad de los datos, garantizar la calidad de éstos y posibilitar la segregación de datos para diferentes propósitos[56]. Quizás habría que añadir la necesidad de que las tecnologías faciliten la reducción de la "generación" misma de los datos, favorezcan la ausencia de discriminación o exclusión cuando no se participe del sistema plenamente y permitan en todo momento la posibilidad de desconexión y olvido[57]. Insistimos, no se trata tanto de proteger datos personales o sensibles, sino la masa informativa relacionada con un individuo, sus bienes o sus interconexiones, que puede ser utilizada para generar perfiles en línea y analizar su ser exponiendo su espacio privado tanto en la dimensión virtual como física de su persona condicionando su interrelación con el mundo.

En todo caso, la filosofía de la *privacy by design* implica mucho más que la implementación de tecnologías que protegen la privacidad. Constituye un paradigma en el que deben confluir el apoyo de la regulación, una supervisión independiente, la responsabilidad y transparencia, la fuerza del mercado, la concienciación de todos los actores, la seguridad de la información, las *Fair Information Practices* y, sólo con todo ello, la adecuada infraestructura tecnológica y operativa[58]. Siempre desde la idea de ruptura con la obsesión por la protección "de los datos personales" para buscar la focalización de las decisiones en la devolución de la verdadera autodeterminación informativa y decisional a las personas.

Se trata de retornar a lo básico y de exigir, como dirá Poullet, que se reduzca la información enviada y recibida a lo estrictamente necesario para lo que persigue el usuario y siempre que éste haya solicitado algún tipo de comunicación[59], no para lo que persiga el mercado o el Estado o los científicos o cualquier "otro".

Y aquí el Derecho no puede permanecer inactivo.

---

55. A este respecto, SCHWARTZ, P. M., "Beyond Lessig'S Code For Internet Privacy: Cyberspace Filters, Privacy-Control, And Fair Information Practices", *Wisconsin Law Review*, 2000, pp. 766-771.

56. Así, SCHAAR, P., "Privacy by Design", cit., p. 273.

57. A este respecto, FINOCCHIARO, G., "La memoria de la rete et il diritto all'oblio", *Il Diritto Dell'Informazione e Dell'Informatica,* vol. XXVI, nº 3, 2010, pp. 391-404.

58. Véase CAVOUKIAN/POLONETSKY/WOLF, "SmartPrivacy for the Smart Grid", cit., p. 276.

59. POULLET, "About the E-Privacy", cit., pp. 27-28.

3. El gran reto del legislador: moldear un "código" propicio para la privacidad que permita transitar de la sensación de protección a la garantía de seguridad

Entendiendo que la configuración actual de la protección legal de la privacidad no resulta plenamente satisfactoria frente a la evolución exponencial de las tecnologías y la creación de una nueva dimensión integral de la persona, que se exterioriza tanto en un mundo "físico" como en un mundo "virtual" cada vez más entrelazados, parece lógico reclamar del legislador la responsabilidad de moldear la arquitectura de la infraestructura tecnológica que nos rodea y exigirle que garantice unos principios mínimos que aseguren el respeto, entre otros, del derecho a la vida privada.

De lo que se trataría es de transitar desde las infraestructuras de vigilancia y trazabilidad a las que sean "amigables" a la privacidad, garantizándose, legalmente, que ello no implique ni exclusión ni discriminación. Aquí es donde el Derecho debe acudir en auxilio de la tecnología para moldear el "código" que configura la infraestructura tecnológica actual a fin de que incorpore parámetros no negociables protectores de la privacidad que permitan a las personas interactuar y transitar de una forma protegida y segura del respeto a sus derechos, a sus elecciones, a su esencia como individuo.

Claro que pueden crearse en el ámbito penal nuevos tipos de lesión o de peligro vinculados con la tutela de intereses tradicionales; por supuesto puede reconocerse la necesidad de tutelar los sistemas de información con propuestas que atiendan la posibilidad de garantizar "nuevos" bienes jurídicos, intermedios o no; podemos también complementar y fortalecer el cumplimiento de los requisitos administrativos del tratamientos de datos con sanciones punitivas. Pero todo ello es insuficiente si no acabamos de comprender el origen de la desprotección de la vida privada y aceptamos como válida, de modo conformista, una tecnología lesiva de ella ya en la propia conceptualización e infraestructura que la soporta.

Como se dice en las conclusiones del Informe MIAUCE "*ha llegado el momento de que la ley también busque la ayuda de la tecnología para asegurar que los mismos instrumentos destinados a la observación de personas y eventos (con fines que van desde la seguridad hasta la comercialización y el entretenimiento; a través de tecnologías que implican la observación y/o la interacción y/o la generación de perfiles) no nieguen a los individuos de forma desproporcionada e ilegítima la protección adecuada de sus derechos y libertades fundamentales*"[60].

Pero, así como no todo puede dejarse a la ley, tampoco todo puede dejarse a la tecnología. Es el legislador el que tiene que definir en este contexto cuáles son los parámetros con los que ha de operar la tecnología. Hasta ahora el legislador ha focalizado su atención en el uso de datos y sistemas. El paso que ha de dar es el de atender también la configuración tecnológica que sustenta ambos.

---

60. CORNELIS, M./DARQUENNES, D./GRANDJEAN, N./LOBET-MARIS, C-/POULLET, Y./ ROUVROY, A., *Deliverable D5.1.2, Ethical, legal and social issues. Multi modal Interaction Analysis and exploration of Users within a Controlled Environment (MIAUCE)*, 2007, p. 125 (en http://www.fundp.ac.be/pdf/publications/70144.pdf).

Y ha de hacerlo incentivando el paradigma de la *privacy by design* y "exigiendo" su aplicación[61], atendiendo los siguientes aspectos: 1º garantizar una generación, recolección y tratamiento mínimo de información sin que ello implique un empeoramiento de la funcionalidad de los servicios recibidos, 2º el parámetro a tomar en cuenta para definir ese "mínimo" debe venir dado por el "propósito" del usuario –no de un tercero-, 3º devolver el "poder" a las personas sobre sus datos (esto implica darles capacidad de auditar, controlar, negar, ocultar, rectificar, acceder, segregar información, volverse anónimo), incluso con un reconocimiento del derecho al olvido digital, 4º reconocer el derecho a la desconexión, sin que esto implique exclusión o discriminación, 5º exigir transparencia en la forma en que funcionan los sistemas y en que recolectan, administran, usan y transmiten la información, haciendo posible verificar su adecuación con la ley y las políticas de privacidad en ellas definidas y auditar su cumplimiento, 6º exigir que por defecto se establezcan las opciones más protectoras de la privacidad, 7º reconocer la existencia de una dimensión virtual y física, personal y privada, de los individuos y la necesidad de protegerla de injerencias e intromisiones no autorizadas, ya sean comunicaciones no solicitadas ya se trate de una vigilancia ubicua con trazabilidad de sus actos en la Web, 8º recordar que el derecho a la vida privada no es "descartable", por lo que deben existir parámetros protectores mínimos y fijos integrados a la tecnología.

Varios de estos aspectos serán difíciles de definir. Especialmente compleja será la concreción de lo que ha de entenderse por espacio público y privado de acción y de en qué medida, aún dentro del "espacio público", determinadas acciones pueden o deben quedar protegidas por el "anonimato" del conjunto[62] frente a la progresiva implementación de ambientes inteligentes[63]. Es aquí donde el legislador está llamado a trazar la línea entre lo que el Derecho no puede permitir y lo que las personas, empoderadas de sus derechos, sí pueden[64].

La incorporación de la protección del derecho a la vida privada a la conceptualización y diseño de la infraestructura tecnológica que nos rodea es una necesidad, pero la concienciación de las personas de los riesgos a valores importantes que surgen de su interacción en el mundo virtual es fundamental. De hecho uno de los principales problemas a los que nos enfrentamos hoy en día es el de la banalización de la exposición de datos en el mundo virtual, de la que deriva la facilidad para recolectar información sin conocimiento del implicado. Es necesario concienciar sobre riesgos y consecuencias. Y es importante crear un espacio de diálogo real y transparente en el que la interacción entre usuarios y servicios y/o productos ofrecidos no sea, como se decía, un "perder-ganar" o un "perder-perder", sino un "ganar-ganar".

Y lo que ha de garantizar el marco normativo es la creación de espacios donde puedan asegurarse unos derechos que no cabe banalizar como parte del intercambio que motoriza la economía digital o la sed de control estatal y en los que no primen los

61. Véase HUSTINX, "Privacy by design", cit., pp. 253 ss.

62. FRIEDMAN, B./HAGMAN, J./KAHN, P. H., "The Watcher and the Watched", cit., pp. 145 ss.

63. CORNELIS *et alter*, *Deliverable D5.1.2*, cit., pp. 87-89.

64. A este respecto, LE MÉTAYER, "Privacy by Design", cit., pp. 329-330.

intereses del mercado o la "oscurantista" pretensión de seguridad estatal. Unos derechos sobre los que se obligue al usuario a pensar en una realidad en que la opción no sea la de "o lo tomas o lo dejas", la de "diga sí para continuar", la de "estoy informado de", cuando no es cierto. No se trata sólo de favorecer la interactuación dentro de esquemas de protección aparentemente respetuosos con la vida privada y transparentes, sino de exigir aquéllos que nos den la absoluta seguridad de que sean cuales sean las decisiones que tomemos, nuestros derechos, irrenunciables, están a salvo, seguridad de que nuestra privacidad, no ya en el momento de la decisión que tomamos, sino en el futuro, no será violada por lo que hayamos decidido, más allá de distinciones entre espacios corporales o incorporales.

¿Con el Derecho penal? También. Son muchas las legislaciones que, siguiendo las recomendaciones u obligaciones internacionales, penalizan el "abuso de dispositivos" que permiten (o con la intención de) cometer delitos contra la confidencialidad, integridad y disponibilidad de los datos, ya sea en cuanto a su creación, en cuanto a su difusión, su uso o cualquier forma de puesta a disposición. ¿Por qué no cabe atender también la posibilidad de sancionar la ausencia de incorporación de la privacidad en el diseño de la infraestructura tecnológica, cuando se sabe que de no incorporarse es imposible que ese derecho (quizás no de forma inmediata) no sufra?

Seguramente no estemos sino comenzando a vislumbrar lo que la tecnología puede hacer, por lo que el principio de neutralidad tecnológica debe permear todos los niveles de tutela jurídica, incluyendo un Derecho penal que no puede cegarse por terminologías atrayentes y discursos pseudo-científicos sin atender cuáles son los intereses realmente en juego. Un Derecho penal que debe poder utilizarse como herramienta para garantizar que en el desarrollo de las nuevas tecnologías se tome en cuenta la tutela de la vida privada desde su diseño como condicionante necesaria para su aceptación. Para, así, asegurar el retorno al usuario del verdadero control sobre su información. Un Derecho penal que permita garantizar que nadie esté obligado a dejarse perfilar, clasificar y codificar bajo amenaza de discriminación o exclusión. Un Derecho penal que garantice la mínima y necesaria generación y recolección de información, la desconexión, el olvido y, en el más amplio sentido de la expresión, el poder ser "dejado en paz".

Esto no tiene que implicar renunciar a la idea de un Derecho penal mínimo. Mínimo pero suficiente. El planteamiento de aquella posibilidad se revela simplemente como opción, quizás única, para evitar la proliferación de tecnologías que, voluntariamente o por negligencia, en su diseño, más que coadyuvar, conducen a la vulneración de la privacidad. ¿Se adelantan con ello las barreras tradicionales de intervención del Derecho Penal? Sin duda. Pero es que es difícil actuar de otro modo aquí, en un ámbito en el que si el Derecho no crea esos espacios amigables aludidos la pérdida de lo que la privacidad conlleva será imposible de evitar.

III. BIBLIOGRAFÍA

BABBITT, R./CHANG, C./YANG, H. I./WONG, J., "Environment Objects: A Novel Approach for Modeling Privacy in Pervasive Computing", *Lecture Notes in Computer Science*, Ambient Assistive Health and Wellness Management in the Heart of the City, vol. 5597, 2009, pp. 166-173.

BURNIK, J./PIRC MUSAR, N., "The Dangers of Electronic Traces: Data Protection Challenges Presented by New Information Communication Technologies", *Lecture Notes in Computer Science, Ethics and Policy of Biometrics*, vol. 6005, 2010, pp. 7-13.

CAVOUKIAN, A., *Privacy by design…take the challenge*, Whasington D.C., 1997.

——, "Privacy by design: the definitive workshop*", Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 247-251.

—— /POLONETSKY, J./WOLF, C., "SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 275-294.

CHARLESWORTH, A./PEARSON, S., "Accountability as a Way Forward for Privacy Protection in the Cloud", *Lecture Notes in Computer Science*, Cloud Computing, vol. 5931, 2009, pp. 131-144.

COLEMAN, S., "E-mail, terrorism and the right to privacy", *Ethics and Information Technology*, vol, 8, nº 1, 2006, pp. 17-27.

CORNELIS, M./DARQUENNES, D./GRANDJEAN, N./LOBET-MARIS, C-/POULLET, Y./ ROUVROY, A., *Deliverable D5.1.2, Ethical, legal and social issues. Multi modal Interaction Analysis and exploration of Users within a Controlled Environment (MIAUCE)*, 2007 (en http://www.fundp.ac.be/pdf/publications/ 70144.pdf).

DE HERT, P./GONZÁLEZ FUSTER, G./GUTWIRTH, S., "Legal safeguards for privacy and data protection in ambient intelligence", *Personal and Ubiquitous Computing,* vol. 13, nº 6, 2009, pp. 435-444.

DEY, A. K./HONG, J. I./LANDAY, J. A./LEDERER, S., "Personal privacy through understanding and action: five pitfalls for designers", *Personal and Ubiquitous Computing*, vol. 8, nº 6, 2004, pp. 440-454.

DÍEZ RIPOLLÉS, J. L., "De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado", *Revista electrónica de ciencia penal y criminología*, nº 7, 2005, pp. 1-36.

DIX, A., "Built-in privacy - no panacea, but a necessary condition for effective privacy protection", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 257-265.

FEDERRATH, H., "Privacy Enhanced Technologies: Methods - Markets - Misuse", *Lecture Notes in Computer Science*, Trust, Privacy, and Security in Digital Business, vol. 3592, 2005, pp. 1-9.

FINOCCHIARO, G., "La memoria de la rete et il diritto all'oblio", *Il Diritto Dell'Informazione e Dell'Informatica,* vol. XXVI, nº 3, 2010, pp. 391-404.

FRIEDMAN, B./HAGMAN, J./KAHN, P. H., "The Watcher and the Watched: Social Judgments about Privacy in a Public Place", *Computer Supported Cooperative Work*, Media Space 20 + Years of Mediated Life, 2009, pp. 145-176.

HUSTINX, P., "Privacy by design: delivering the promises", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 253-255.

INFORMATION AND PRIVACY COMMISSIONER/REGISTRATIERKAMER, *Privacy-Enhancing Technologies: The Path to Anonymity*, vol. I y II, 1995 (en http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf).

JENSEN, C. D./SEIGNEUR, J. M., "Trading Privacy for Trust", *Lecture Notes in Computer Science*, Trust Management, vol. 2995, 2004, pp. 93-107.

JOHNSON-PAGE, G. F./THATCHER, R. S., "B2C data privacy policies: current trends", *Management Decision*, vol. 39, nº 4, 2001, pp. 262-271.

JUTLA, D. N., "Layering privacy on operating systems, social networks, and other platforms by design", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 319-341.

KÖFFEL, C./WÄSTLUND, E./WOLKERSTORFER, P., "PET-USES: Privacy-Enhancing Technology - Users' Self-Estimation Scale", *IFIP Advances in Information and Communication Technology*, vol. 320, Privacy and Identity Management for Life, 2010, pp. 266-274.

KOORN RE, R. (Editor), *Privacy-Enhancing Technologies, White Paper for Decision-Makers*, Ministry of the Interior and Kingdom Relations, Netherlands, 2004.

KOTZANIKOLAOU, P./MAGKOS, E., "Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments", *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 1, vol. 47, Security and Privacy in Mobile Information and Comunication Systems, Part 2, pp. 53-64.

LE MÉTAYER, D., "Privacy by Design: A Matter of Choice", *Data Protection in a Profiled World,* Part 6, 2010, pp. 323-334.

___ /MONTELEONE, S., "Automated consent through privacy agents: Legal requirements and technical architecture", *Computer Law & Security Review*, vol. 25, nº 2, 2009, pp. 136-144.

LANGHEINRICH, M., "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems", *Lecture Notes in Computer Science,* Ubicomp, vol. 2201, 2001, pp. 273-291.

LEIGHTON, P., "Uso excesivo de las redes sociales tiende a borrar el límite entre lo público y lo privado", *El Mercurio*, Chile, 25 de junio de 2011, p. A14.

LESSIG, L., *Code: and other laws of Cyberspace*, version 2.0 Basic Books, New York, 2006.

McADAMS, A. J., "Review: Internet Surveillance after Septembre 11: is the United States becoming GreatBritain?", *Comparative Politics*, vol. 37, nº 4, 2005, pp. 479-498.

ORTIZ PRADILLO, J. C., "El 'Remote Forensic Software' como herramienta de investigación contra el terrorismo", *INTECO-Formación, Estudios e Informes ENAC,* nº 4, 2009, pp. 1-9.

PEARSON, S./YUN, S., "Context-Aware Privacy Design Pattern Selection", *Lecture Notes in Computer Science*, Trust, Privacy and Security in Digital Business, vol. 6264, 2010, pp. 69-80.

PEISSL, W., "Information Privacy in Europe from a TA Perspective", *Data Protection in a Profiled World*, London, 2010, pp. 247-256.

POULLET, Y., "About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?", *Data Protection in a Profiled World*, London, 2010, pp. 3-30.

SCHAAR, P., "Privacy by Design", *Identity in the Information Society*, vol. 3, nº 2, 2010, pp. 267-274.

SCHWARTZ, P. M., "Beyond Lessig'S Code For Internet Privacy: Cyberspace Filters, Privacy-Control, And Fair Information Practices", *Wisconsin Law Review*, 2000, pp. 743-788.

___, "Internet Privacy and the State", *Connecticut Law Review*, vol. 32, 2000, pp. 815-859.

___, "Privacy, Ethics, and Analytics", *IEEE Security & Privacy*, mayo/junio 2011, pp. 66-69.

SMITH, J./PROSCH, M, "Extending the value chain to incorporate privacy by design principles", *Identitiy in the Information Society*, vol. 3, nº 2, 2010, pp. 295-318.

VAN DEN HOVEN, J., "The Tangled Web of Tiny Things: Privacy Implications of Nano-electronics", *Nanotechnology & Society*, nº 3, 2009, pp. 147-162.