José Luis Piñar Mañas*

SOCIEDAD, INNOVACIÓN Y PRIVACIDAD**

La innovación es constante en la historia de la humanidad. Las tecnologías disruptivas no son exclusivas de nuestro tiempo. Lo peculiar de ahora es que la innovación puede autogenerar conocimiento e inteligencia. Es decir, la propia innovación, o mejor el resultado de la innovación, se autonutre de sus propios avances tecnológicos, y en un escenario en el que el tratamiento, a veces masivo, de datos personales es imprescindible. Esto exige interrogarse acerca de la pervivencia o no de la privacidad. ¿Podemos entender que existe todavía la privacidad? La respuesta debe ser afirmativa. Y para ello el Derecho desempeña un papel capital. Derecho e innovación no son incompatibles, sino que pueden y deben convivir, partiendo siempre de la importancia que tiene basar la protección de la privacidad en principios jurídicos fundamentales que tengan en cuenta los elementos esenciales de la relación entre privacidad e innovación en la sociedad actual. Principios que partan de la configuración de la protección de datos como parte de la dignidad humana que no admite su mera patrimonialización económica.

Palabras clave: *tecnologías disruptivas, protección de datos, inteligencia artificial,* big data.
Clasificación JEL: *K23, K24, K38, O33, O35.*

1. Sociedad e innovación

Pocas veces como ahora se habla de la innovación en la sociedad. Pareciera que las tecnologías disruptivas fuesen propias y exclusivas de nuestra época.

Pero los cambios radicales, disruptivos, han estado siempre presentes en la historia de la humanidad. Sin remontarnos a momentos demasiado lejanos bastaría con referirnos a un acontecimiento tan sublime y radicalmente innovador como la Revolución Francesa. No hace mucho (Piñar Mañas, 2017, 14 y ss.) recordaba que García de Enterría ya expuso magistralmente hace años cómo la Revolución Francesa «fue un tajo decisivo entre lo que a partir de entonces se llamaría, muy justamente, el Antiguo Régimen y el nuevo orden político y social que pretendió crearse sobre fundamentos enteramente nuevos» (1994, 18). Todo cambió a partir de entonces, y el Derecho hubo de adaptarse a ello. Con la Revolución Francesa «toda la representación del mundo social y colectivo cambió súbitamente. La vieja y rígida estructura social fue rasgada de un solo golpe» (1994, 26). Y así como ahora

* Catedrático de Derecho Administrativo. Abogado. Director del Máster Universitario en Protección de Datos, Transparencia y Acceso a la Información y Titular de la Cátedra Google sobre Privacidad, Sociedad e Innovación de la Universidad CEU San Pablo de Madrid.

** El presente trabajo se enmarca en el proyecto de investigación *Protección de datos, seguridad e innovación: retos en un mundo global tras el Reglamento Europeo de Protección de Datos*, referencia DER2016-79819-R, de la Convocatoria 2016 de Proyectos de I+D+i, del Ministerio de Economía y Competitividad, del que soy investigador principal.

hemos de acostumbrarnos a marchas forzadas a un nuevo lenguaje dictado desde la técnica, también entonces surgió un nuevo léxico, pero desde la sociedad y el Derecho: «la Revolución fue... desde sus orígenes... una guerra de palabras» (1994, 27). Surge así un nuevo lenguaje jurídico, la «lengua de los derechos», explicada «no como una simple aparición de nuevos términos, en un plano estrictamente técnico de análisis léxico o sintáctico, sino como la expresión de un nuevo discurso jurídico que ofrece un nuevo modelo de relación entre los hombres» (1994, 37).

En el paso del Siglo XIX al XX se dieron las condiciones para que, a partir de no pocos «acontecimientos desencadenantes», se produjese una «aceleración de la historia» (Remaud, 2007, 99; Casullo, 2017, 66). La modernidad, que tuvo entre otros referentes la inimaginable transformación que experimentó París a partir de las ideas y proyectos de Haussmann a mediados del Siglo XIX, «es lo transitorio, lo fugitivo, lo contingente... que (sin embargo) nadie tiene derecho a despreciar o ignorar» (Baudelaire, traducción de 2007, 92). La modernidad supone pues cambios radicales, como los que se experimentaron a principios del pasado siglo, cambios que hoy también podemos considerar disruptivos.

En consecuencia, no podemos considerar que solo ahora se «acelere la historia». Si bien la velocidad del cambio es hoy mucho más intensa que lo que ha sido en cualquier otro momento de la historia de la humanidad. Como ya señalé en otra ocasión (Piñar Mañas, 2009), la evolución hoy está siendo extraordinariamente rápida y profunda, lo que permite hablar de verdadera revolución. Tan rápida, que «cualquier relato de ese tipo (sobre la historia de la revolución de la tecnología de la información) quedaría obsoleto de inmediato» (Castells, 2005, 70). Como ha señalado expresivamente Clippinger (2007, 24), «el cambio es tan rápido que ningún día guarda relación significativa con el anterior». Además, el actual escenario tiene elementos que nos presentan un decorado cualitativamente diverso; y ello fundamentalmente por la aparición de un actor nuevo que trastoca el relato que hasta ahora iba desarrollándose.

Ese actor son las tecnologías de la información y de la comunicación (o del conocimiento, según expresión también utilizada): tecnologías que pueden autogenerar conocimiento e inteligencia. Es decir, la propia innovación, o mejor, el resultado de la innovación, se autonutre de sus propios avances, con lo que esto puede suponer. Además el cambio es constante, y «en torno a él gira el mundo moderno» (Kelly, 2017, 5). Cambio que requiere imprescindiblemente, hoy por hoy, de Internet. La Red se convierte, se ha convertido hace años, en la clave de bóveda de la innovación tecnológica que transforma la sociedad. Con indudables e irrenunciables avances para la entera sociedad, a nivel planetario. Lo que sin embargo y por otro lado, como he señalado ya en otro lugar (Piñar Mañas, 2017, 15), implica no pocas amenazas para los derechos, y en particular para la privacidad o la protección de datos de carácter personal (Castells, 2005, 70). Al mismo tiempo implica la necesidad de configurar nuevos derechos, los de los llamados ciudadanos digitales (Solove, 2004) o de la ciudadanía digital (Rodotà, 2014), que buscan reconocer los nuevos derechos que esta nueva situación trae consigo. No es aventurado afirmar que en un futuro no muy lejano la vida cotidiana de gran parte de la población (no la de unos pocos) va a estar condicionada por el uso de la innovación tecnológica y en particular de Internet. La práctica totalidad de las manifestaciones de la vida cotidiana van a estar directa o indirectamente vinculadas a Internet. Una Internet que debe ser necesariamente neutral (Fuertes, 2015), y respecto de la que desde hace ya tiempo (Villar Palasí, 1998) se ha debatido la necesidad o no de su regulación (Muñoz Machado, 2000).

Kevin Kelly ha analizado los modos en que «de forma habitual» las «personas medias» están sujetas a una vigilancia constante: desde los drones a la videovigilancia; desde las tarjetas de fidelización a las redes sociales; desde los buscadores a las aplicaciones (Kelly, 2017, 248-250). La monitorización y seguimiento de las personas es cada vez más intensa. Y lo grave

es que pese a que cada vez somos más conscientes de ello, lo cierto es que la vigilancia sigue pasando desapercibida. Vuelve incluso a recuperarse la idea del panóptico de Jeremy Bentham, esa cárcel cuyo diseño permite al carcelero vigilar a todos los reclusos sin que estos sepan siquiera que están siendo observados, lo que haría de ellos dóciles sujetos, al saberse constantemente vigilados. Idea que más adelante teorizó Foucault (1976) como forma de vigilancia constante y control social y que ya se ha relacionado con la era de la innovación (King, 2001). Se habla del panóptico «vigilancia total**»** (Whitaker, 1999). Algo que la tecnología puede hacer realidad (Holtzman, 2006, 265). Como Jeffrey Rosen (2000) ha señalado, estamos sometidos a una «mirada no deseada**»**, que puede destruir nuestra privacidad. Baker (2009, 19) ha advertido que los matemáticos y científicos de la computación poseen el poder de controlar la información de nuestra vida. Sofsky (2009) ha denunciado la existencia de una vigilancia sin fisuras. Una «vigilancia líquida**»** en una fase «pospanóptica**»** (Bauman y Lyon, 2013).

Ante este riesgo o amenaza de vigilancia constante, Rodotà (2014b) ha hablado con razón del «derecho a hacer silencioso el chip», el derecho «a desactivar el chip contenido en un *gadget* o en cualquier otro dispositivo que la persona lleve consigo o que se encuentre en su auto o en su casa, interrumpiendo de este modo la transmisión de datos a un sujeto determinado». Las tecnologías de la información deben estar al servicio de la persona, no fagocitarla. El ser humano, al menos en su relación con los poderes públicos, debe beneficiarse de la innovación tecnológica aunque él mismo decida permanecer al margen de dicha innovación, en general o en relación con extremos que considere amenazantes para sus derechos, muy en particular su derecho a la privacidad o protección de datos. No debe ser necesario «cosificar» a la persona o convertirla en una base de datos para que pueda desarrollar sus opciones vitales en la ciudad o fuera de ella (Piñar Mañas, 2017).

En cualquier caso, y sin perjuicio del derecho a la desconexión al que antes me refería, lo cierto es que la innovación hace que el futuro de la sociedad sea digital, en el que podrá llegarse a una conectividad casi completa. Rodotà (2017) ha señalado que «muchas transformaciones justifican la consideración del hombre como un nuevo objeto conectado», presentado incluso como una «nano-bio-info-neuro-máquina», recordando al «hombre maquina» del que en el Siglo XVIII hablaban La Mettrie y D'Holbach. Futuro digital en el que junto a la identidad física convivirá la identidad virtual, *online*: «en el futuro la identidad será la materia prima más valiosa para los ciudadanos y esta existirá principalmente *online*» (Schmidt y Cohen, 2014).

Ahora bien, esa identidad *online* puede llegar a ser definida no desde la autonomía de la persona sino heterónomamente. El poder de los algoritmos puede configurar la identidad de la persona, una identidad controlada, diseñada y vigilada. Lo que pone en cuestión el propio derecho al libre desarrollo de la personalidad. Una identidad cuya configuración puede limitarse, en base al modo en que se reconducen e incluso definen los gustos o prioridades de las personas. Se puede perfilar con facilidad a las personas y puede limitarse el marco de su desarrollo personal en un proceso difícil de identificar y ante el que puede resultar aún más difícil resistirse, pues en definitiva el algoritmo va a adecuar procesos a nuestros gustos, por lo que no será fácil objetar las indicaciones que de ello se deriven. Pero al mismo tiempo puede cercenar la apertura y diversificación de la personalidad y por tanto de la propia identidad, pues en definitiva se va empobreciendo la capacidad de apertura a lo diverso y nuevo. Dicho con otras palabras y, por ejemplo, si en base a nuestros gustos y de acuerdo a técnicas de *online behavioral advertising* (publicidad comportamental en línea) se nos muestran y ofrecen productos (de todo tipo, música, ocio, viajes, consumo…) que encajan o coinciden con nuestras preferencias como consecuencia del seguimiento que se hace de nuestra vida en Internet, lo cierto es que con gran probabilidad nos sentiremos cómodos con lo que se nos ofrece, pero se cerrará o al menos no se facilitará el acceso a

otros productos que pueden enriquecer nuestra personalidad. Lo que a largo plazo y de forma casi desapercibida puede llegar a condicionar e incluso definir desde fuera la personalidad del ser humano, que poco a poco pasa a ser más controlable y maleable.

Porque en realidad la mayor parte de las innovaciones tecnológicas que están produciéndose en la actualidad tienen directa (las más de las veces) o indirecta relación con el tratamiento de datos de carácter personal. Ya hace años se habló de las RFID, las *cookies* o más recientemente del *cloud computing*. Hablamos ahora también de *big data,* Internet de las cosas*, wearables, bitcoin, block chain,* robótica*,* drones, inteligencia artificial*, gene drive technology, data driven innovation,* ciudades inteligentes… Cualquiera de estos conceptos es imposible sin el uso de datos. En particular la inteligencia artificial. Bostrom (2016, 19) nos recuerda que Nilsson (2009), uno de los más importantes expertos en inteligencia artificial, considera que la llegada de la inteligencia artificial de nivel humano puede producirse entre 2030 y 2100.

Todo ello pone en el centro del debate los datos personales. Y la gran duda: ¿es posible en este escenario de innovación constante mantener la privacidad? Hace ya años me preguntaba si realmente existe la privacidad (Piñar Mañas, 2010).

2. Privacidad

Como digo, los grandes retos y al mismo tiempo los grandes avances de la sociedad pasan por el tratamiento de datos personales. No solo los avances de la ciencia, sino los retos de la falta, cierta o no, de seguridad. Los primeros no son posibles sin el manejo de datos. La garantía de la segunda parecería exigir el tratamiento masivo de datos e información. Lo que ha llevado a muchos a preguntarse sobre el futuro, e incluso el presente, de la privacidad. Paissan (2009) ha escrito que «la privacidad está muerta», Wacks (2010, 132) también se pregunta si estamos ante la muerte de la privacidad, Mills (2008) se refiere a la privacidad como «el derecho perdido», Rubenfeld (2008) habla del fin de la privacidad.

¿Es posible reaccionar ante esta situación desoladora pero no lejana a la realidad, en la que la protección de datos desaparece? En mi opinión sí. Ante las reflexiones constantes en relación con las graves amenazas a las que la protección de datos está hoy sometida no es difícil constatar que la privacidad se ha convertido en uno de los derechos protagonistas de la sociedad de nuestros días, y parece que va a seguir siéndolo durante no poco tiempo. Los ciudadanos cada vez valoran más su privacidad y el derecho y los tribunales no dudan en dar a la protección de datos el impulso que merece y necesita.

Resulta en cualquier caso imprescindible reivindicar el derecho a la protección de datos, manifestación de la dignidad de la persona (en mi opinión, y pese a que se ha planteado ya desde hace años la posibilidad de reconocer el derecho a la privacidad de los grupos, y teniendo en cuenta que privacidad y protección de datos no son del todo coincidentes, la protección de datos ha de reconocerse solo a las personas físicas. Véase en relación con la privacidad de los grupos Bloustein, 2003 y Floridi, 2014). Rodotà (2014) lo ha recordado y advertido reiteradamente: «La dignidad… evita que la persona sea considerada como una especie de explotación a cielo abierto en la que cualquiera puede recoger información y construir perfiles… que convierten a la persona en objeto de poderes externos, que pueden falsificarla, construirla de formas coherentes con las necesidades de una sociedad vigilada, de la selección social, del cálculo económico». Y en este sentido debe llamarse la atención sobre ciertos intentos de reducir los datos personales a simple moneda de cambio, considerándolos como contraprestación por el suministro de contenidos digitales, que podrían pagarse no ya con dinero, sino con datos. El artículo 3.12 de la propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales afirma que dicha Directiva «se aplicará a cualquier contrato en virtud del cual el

proveedor suministra contenidos digitales al consumidor o se compromete a hacerlo y, a cambio, se paga un precio o el consumidor facilita activamente otra contraprestación no dineraria en forma de datos personales u otro tipo de datos». El Supervisor Europeo de Protección de Datos[1], en su Dictamen 4/2017 advierte con razón «contra (…) la idea de que los ciudadanos pueden pagar con sus datos del mismo modo que con su dinero. Derechos fundamentales como el derecho a la protección de los datos personales no pueden quedar sometidos al puro interés de los consumidores, como tampoco deben considerarse los datos personales como una mera mercancía».

Esta es en mi opinión la línea correcta. La innovación puede llegar a cosificar a la persona, someterla a la sola tecnología del algoritmo (Rodotà, 2017). Pero también el desarrollo de la sociedad en un escenario de nuevos y cada vez más sofisticados servicios basados en la obtención y tratamiento de datos puede llegar a cosificar al ser humano, a convertirlo en un simple conjunto de datos que pueden obtenerse con extrema facilidad incluso con el conocimiento y el consentimiento de los afectados, que se someten voluntariamente a una suerte de despojo de su personalidad, sin ser conscientes de las consecuencias que de ello pueden derivar. La persona se hace ella misma transparente, en una transparencia casi pornográfica (Han, Byung-Chul, 2014).

Y, como decía, el Derecho reacciona con decisión. El 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 y por el que se deroga la Directiva 95/46/CE: Reglamento General de Protección de Datos (*DOUE* L 119, de 4-5-2016), que será plenamente aplicable a partir del 25 de mayo de 2018, supone la apuesta europea por el máximo respeto a la protección de datos. Y ello en base al reconocimiento que de tal derecho contiene el artículo 8 de la Carta Europea de los Derechos Fundamentales:

— Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

— Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

— El respeto de estas normas quedará sujeto al control de una autoridad independiente.

El Reglamento, que es una de las normas europeas que más debates ha generado durante su proceso de elaboración y de las que más presiones ha recibido por *lobbies* de todo tipo y origen, supone el cambio a un nuevo modelo de protección de datos (Piñar Mañas, 2016) que está llamado a ser la referencia global en protección de datos. No solo por la influencia que el texto pueda tener en los marcos y desarrollos normativos de no pocos países, sino por la extraordinaria amplitud de su ámbito de aplicación territorial. El artículo 3.2 señala en efecto que el Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: *i)* la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o *ii)* el control de su comportamiento, en la medida en que este tenga lugar en la Unión. Es decir, las más grandes empresas multinacionales que basan en el tratamiento de datos gran parte de su actividad (Google, Facebook, Amazon, Microsoft, Linkedin, Yahoo, y tantas otras) van a tener que adaptarse obligatoriamente al nuevo Reglamento Europeo antes del 25 de mayo de 2018. Ya solo esta consecuencia es de un alcance y trascendencia hasta ahora desconocidos. Y se inscribe en un proceso de globalización de la

[1] Supervisor Europeo de Protección de Datos (2017). *Dictamen 4/2017, sobre la propuesta de Reglamento relativo a la privacidad y las comunicaciones electrónicas (Reglamento ePrivacy)*, disponible en *www.edps.europa.eu*. En el DOUE de 20 de julio de 2017, nº C 234, se publica un resumen ejecutivo en español (el original del Dictamen se ha publicado en inglés, francés y alemán).

protección de datos que va consolidándose sin pausa en los últimos años.

Dicha globalización es imprescindible para conseguir que la tutela de la protección de datos no se quede en meras palabras o buenas intenciones. En este sentido la creación por Naciones Unidas de un relator especial para el derecho a la privacidad (Resolución del Consejo de Naciones Unidas de Derechos Humanos A/HRC/28/L.27 de 24 de marzo de 2015 por la que se establece dicho relator especial) debe ser bien recibida, pero no es suficiente. Por otra parte, no faltan voces que se muestran escépticas ante lo que el Derecho puede hacer en favor de la privacidad. Bennett y Raab (2006) consideran que las leyes de protección de la privacidad y de protección de datos solo pueden tener un «impacto marginal» en el desarrollo de la sociedad de la vigilancia. Holtzman (2006, 119) considera que las leyes de protección de datos «no funcionan particularmente bien». Rule (1980) considera incluso que en no pocas ocasiones las leyes que regulan el derecho a la privacidad son utilizadas para legitimar la introducción de nuevos sistemas de vigilancia. Laperrière (citado por Bennett y Raab, 2006, 147) ha señalado que la legislación de protección de datos parece una solución del pasado. Gellman se ha preguntado directamente si el derecho a la privacidad realmente funciona.

Ante estas pesimistas posturas creo firmemente que el Derecho ocupa una posición insustituible en la efectiva protección de la privacidad. La evolución del derecho a la privacidad y a la protección de datos, desde Cooley (1888) y Warren y Brandeys (1890) hasta nuestros días, ha sido imparable e incuestionable. Y ha ayudado a impulsar la protección de datos a nivel global.

En este sentido son de extraordinaria importancia diversas sentencias del Tribunal de Justicia de la Unión Europea que afectan directamente a grandes multinacionales y que decididamente advierten que la normativa europea de protección de datos tiene un alcance tal que no está dispuesta a que la defensa de la privacidad ceda cuando los tratamientos de datos puedan llevarse a cabo desde fuera de las fronteras europeas. Me refiero por un lado a la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, asunto C-131/12 (Google Spain, S.L. y Google Inc. vs. Agencia Española de Protección de Datos y Mario Costeja González), en la que, como es sabido, se exige a Google Inc. que atienda el derecho al olvido de una persona que lo solicita en España (ver, entre otros, Alvarez Caro, 2015). Por otro, a la Sentencia del mismo Tribunal de 6 de octubre de 2015, asunto C-362/14, (Maximillian Schrems) por la que se declara inválida la Decisión 2000/520/CE de la Comisión Europea, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro; sentencia que trae causa de una reclamación relacionada con la transferencia de datos a Estados Unidos por parte de Facebook. Es decir, el Tribunal de Justicia no se ha detenido a la hora de enfrentarse a asuntos que tenían directa relación con el tratamiento de datos llevado a cabo por dos de las más importantes compañías del mundo, quizá las que más datos personales manejan, con múltiples posibilidades de afectar a la privacidad de las personas. Ambas sentencias, junto con la de 8 de abril de 2014, asunto C-594/12 (Digital Rights Ireland), por la que se declara inválida la Directiva 2006/24/CE, de retención de datos (el Tribunal Constitucional alemán ya había dictado antes la Sentencia de 2 de marzo de 2010 por la que declaró la inconstitucionalidad de la Ley de 21 de diciembre de 2007, de reforma del control de las telecomunicaciones y para la transposición de la Directiva 2006/24/CE), son una prueba palpable de lo que antes comentaba, de esa apuesta por una protección global de la privacidad.

En cualquier caso, nunca se debe bajar la guardia. La innovación avanza a tal velocidad que el Derecho es muchas veces incapaz de seguirla. La tensión entre ciencia y derecho (Esteve, 2009; Rodotà, 2010) debe solventarse desde la premisa de que innovación y derecho no son en absoluto incompatibles (Recio, 2016). Lo que entonces resulta imprescindible, para no perder la batalla, es tener muy presente que la protección de la privacidad ha de plantearse no desde el intento muchas veces infructuoso de dar respuesta concreta a situaciones coyunturales, repentinas e imprevisibles (recordemos que ya

Baudelaire afirmaba que la modernidad es lo transitorio, lo fugitivo, lo contingente), sino de formular principios que sean capaces de hacer frente a las situaciones que puedan ir presentándose. Este fue ya el principal reto que quiso afrontar Westin (1967) cuando se refirió a la idea de *self determination* como criterio clave de la privacidad. De donde surge el concepto de autodeterminación informativa (Lucas Murillo de la Cueva, 1990 y 2009). Control sobre la propia esfera privada que constantemente ha resaltado Rodotà (proximamente, 2017).

Tales principios han de garantizar frente a cualquier cambio o innovación tecnológica que la protección de datos consiste en la atribución de un poder de disposición sobre los propios datos de carácter personal (lo que se compadece mal, por cierto, con la configuración del dato como «moneda de cambio», tal como vimos anteriormente), de modo que, como ya afirmara nuestro Tribunal Constitucional en su famosa Sentencia 292/2000, de 30 de noviembre (fundamento jurídico séptimo), la persona pueda «decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso». De este modo el derecho a la protección de datos no solo no supondrá un obstáculo para la innovación sino que facilitará su desarrollo. Principios como privacidad desde el diseño y por defecto (hoy recogidos expresamente en el artículo 25 del Reglamento General de Protección de Datos) se definen como fundamentales para el respeto efectivo de la protección de datos.

Lo anterior no debe hacernos olvidar, sin embargo, que los retos de la privacidad en la sociedad actual, testigo de un proceso de innovación como nunca antes se había producido en la historia de la humanidad (no por no haberse producido antes acontecimientos disruptivos sino por la naturaleza misma de la innovación, generadora de conocimiento e inteligencia) son constantes y a veces extraordinariamente graves. Más aún por el hecho de que la tan reiterada innovación se basa en no pocas ocasiones en masivos tratamientos de datos que permiten una vigilancia casi constante. Hoy es perfectamente posible encontrar una aguja en un pajar, siendo la primera el ser humano y el segundo la multitud. Referirse a las técnicas que lo permiten (*face recognition*, geolocalización, lectura de labios a distancia, videovigilancia, *cookies*, retención de datos, Internet de las cosas, etc…) sería fácil y al mismo tiempo poco útil, por la obsolescencia de las mismas y la sustitución casi constante de nuevos avances que incrementan la posibilidad de control en relación con las anteriores. Como he señalado en otro lugar (Piñar Mañas, 2017), la innovación tecnológica es imparable. Y se inserta en la vida cotidiana con extraordinaria rapidez. ¿Dónde está el límite de la innovación? ¿Qué capacidad tiene el ser humano de adaptarse a lo nuevo y de asumirlo como irreversible, de ahí a hacerlo imprescindible y por fin normal? Pongamos el caso de la geolocalización: si en un principio se consideró como un atentado a la privacidad, hoy empieza a ser para muchos algo de lo que es difícil prescindir sin detenerse a pensar en las consecuencias que puede revestir para la protección de datos. La solución no puede ser paralizar la innovación ni obviar el derecho. Muy al contrario, lo que procede es impulsar el dialogo entre derecho y técnica y tener presentes los principios esenciales de los derechos fundamentales, en particular, en lo que ahora nos interesa, de la protección de datos.

Referencias bibliográficas

[1] ALVAREZ CARO, M. (2015). *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*. Madrid: Editorial Reus.

[2] BAKER, S. (2009). *Numerati. Lo saben todo de ti,* Barcelona: Seix Barral.

[3] BAUDELAIRE, CH. (2007). *El pintor de la vida moderna*. Colección de Arquitectura. Colegio Oficial de Aparejadores y Arquitectos Técnicos de la Región de Murcia: Murcia (la obra es traducción del texto original de 1868).

[4] BAUMAN, Z. y LYON, D. (2013), *Vigilancia líquida*, Barcelona: Paidós.

[5] BENNETT y RAAB (2006). *The Governance of Privacy. Policy Instruments in Global Perspective*. Cambridge-Londres: The MIT Press.

[6] BENTHAM, J. (1979). *El Panóptico*. Las Ediciones de La Piqueta, Madrid. disponible en *https://iedimagen.*

files.wordpress.com/2012/02/bentham-jeremy-el-panoptico-1791.pdf

[7] BLOUSTEIN, E. J. (2003). *Individual & Group Privacy* (2ª ed.). New Brunswick, N.J.: Transaction Publishers (1ª ed.1978).

[8] BOSTROM, N. (2016). *Superinteligencia. Caminos, peligros, estrategias*. Teell Editorial, S.L.

[9] CASTELLS, M. (2005). *La era de la información. Vol. 1, La sociedad red*, Madrid: Alianza Editorial, 3ª ed.

[10] CASULLO, N.; FORSTER, R. y KAUFMAN, A. (2017). *Itinerarios de la modernidad*, Buenos Aires: Eudeba.

[11] CLIPPINGER, J.H. (2007). *A Crowd of One. The Future of Individual Identity*. Nueva York: Public Affairs.

[12] COOLEY, T.M. (1888). *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, Chicago: Callaghan 2ª ed. (Disponible en *http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1010&context=books*)

[13] ESTEVE PARDO, J. (2009). *El desconcierto del Leviatán. Política y derecho ante las incertidumbres de la ciencia*, Madrid: Pons.

[14] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2014). *Handbook on European Data Protection Law*, Luxemburgo: Publications Office of the European Union.

[15] FLORIDI, L. (2014). «Open Data, Data Protection, and Group Privacy», *Philosophy & Technology*. Vol. 27, nº 1, marzo 2014, pp. 1-3. También puede consultarse en *https://link.springer.com/content/pdf/10.1007%2Fs13347-014-0157-8.pdf*

[16] FOUCAULT, M. (1976). *Vigilar y castigar*, México: Ed. Siglo XXI.

[17] FUERTES, M. (2015). *Neutralidad de la Red ¿Realidad o utopía?* Madrid: Pons.

[18] GARCÍA DE ENTERRÍA, E. (1994). *La lengua de los derechos. La formación del Derecho Público europeo tras la Revolución Francesa*, Madrid: Alianza Universidad.

[19] GELLMAN (1998). «Does Privacy Law work?» En AGRE y ROTENBERG (Eds.). *Technology and Privacy: The New Landscape*, Londres: The MIT Press.

[20] HAN, B-CH. (2014). *La sociedad de la transparencia.* Barcelona: Herder.

[21] HOLTZMAN, D.H. (2006). *Privacy Lost. How Technology is endangering your Privacy,* San Francisco: Jossey-Bass.

[22] KING, L. (2001). «Information, Society and the Panopticon». *The Western Journal of Graduate Research*, vol. 10, nº 1, pp. 40-50.

[23] LUCAS MURILLO DE LA CUEVA, P. (1990). *El derecho a la autodeterminación informativa*, Madrid: Tecnos.

[24] LUCAS MURILLO DE LA CUEVA, P. y PIÑAR MAÑAS, J. L. (2009). *El derecho a la autodeterminación informativa*. Madrid: Fundación Coloquio Jurídico Europeo.

[25] MILLS, J.L. (2008). *Privacy, the Lost Right*. Nueva York: Oxford University Press.

[26] MUÑOZ MACHADO, S. (2000). *La regulación de la Red, poder y derecho en Internet*, Madrid: Taurus.

[27] NILSSON, N. J. (2009). *The Quest for Artificial Intelligence: A History of Ideas and Achievements*. Nueva York: Cambridge University Press.

[28] PAISSAN, M. (2009). *La Privacy è morta, viva la privacy*, Milán: Ed. Ponte alle Grazie.

[29] PIÑAR MAÑAS, J.L. (2009). *Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio*. Madrid: Fundación Alternativas.

[30] PIÑAR MAÑAS, J.L. (2010). «¿Existe la privacidad?», en *Protección de datos personales. Compendio de lecturas y legislación*. Ciudad de México: IFAI, Cámara de Diputados. Pp. 15-55. Recoge la obra del mismo título publicada en 2008, Madrid: CEU Ediciones.

[31] PIÑAR MAÑAS, J.L. (Dir.) (2014). *Transparencia, acceso a la información y protección de datos*. Madrid: Editorial Reus.

[32] PIÑAR MAÑAS, J.L. (Dir.); ALVAREZ CARO, M. y RECIO GAYO, M. (Coords.) (2016). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Madrid: Editorial Reus.

[33] PIÑAR MAÑAS, J.L. (Dir.); SUAREZ OJEDA, M. (2017). *Smart Cities: derecho y técnica para una ciudad más habitable*, Madrid: Editorial Reus.

[34] RECIO, M. (2016). *Protección de datos personales e innovación: ¿(in)compatibles?*, Madrid: Editorial Reus.

[35] REMAUD, O. (2007). «Pequeña filosofía de la aceleración de la historia». *Isegoría. Revista de Filosofía Moral y Política*, nº 37, julio-diciembre, 2007, pp. 97-111.

[36] RODOTÀ, S. (2010). *La vida y las reglas. Entre el derecho y el no derecho*. Madrid: Trotta.

[37] RODOTÀ, S. (2014 a). *El derecho a tener derechos*, Madrid: Trotta.

[38] RODOTÁ, S. (2014 b). *Il mondo nella rete. Quali i diritti, quali i vincoli*. Roma-Bari: Editorial Laterza.

[39] RODOTÀ, S. (2017). *Dall'umano al postumano*. Ejemplar original entregado por el autor (será próximamente publicado).

[40] ROSEN, J. (2000). *The Unwanted Gaze. The Destruction of Privacy in America*, Nueva York: Vintage Books.

[41] RUBENFELD, J. (2008). «The End of Privacy», *Stanford Law Review*, vol. 61, nº 1, pp. 101-162.

[42] RULE *ET AL*. (1980). *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*. Nueva York: Elsevier.

[43] SCHMIDT, E. y ROSENBERG, J. (2014). *How Google Works*. Londres: John Murray (Publishers).

[44] SCHMIDT, E. y COHEN, J. (2014). *El futuro digital*, Madrid: Ediciones Anaya.

[45] SOFSKY, W. (2009). *Defensa de lo privado*, Valencia: Pre-Textos.

[46] SOLOVE, D. (2004). *The Digital Person. Technology and Privacy in the Information Age*, Nueva York: New York University Press.

[47] TAO, T.; DE CREMER, D. y CHUNBO, W. (2017). *Huawei. Leadership, Culture, and Connectivity*, Nueva Delhi: SAGE Publications.

[48] VILLAR PALASÍ, J.L. (1998). «Implicaciones jurídicas de Internet». *Anales*, Madrid: Real Academia de Jurisprudencia y Legislación.

[49] WACKS, R. (2010). *Privacy. A Very Short Introduction*, Nueva York, Oxford University Press.

[50] WARREN, S. y BRANDEIS, L. (1890). «The Right to Privacy (The Implicit Made Explicit)». *Harvard Law Review,* vol. IV, 15 de diciembre de 1890, nº 5. Hay edición en español: *El derecho a la intimidad* (1995), Madrid: Cívitas.

[51] WESTIN, A.F. (1967). *Privacy and Freedom*, Nueva York: Atheneum, New York.

[52] WHITAKER, R. (1999). *The End of Privacy: How Total Surveillance is Becoming a Reality*. New York: The New Press. Existe traducción al español: *El fin de la privacidad. Cómo la vigilancia total se está convirtiendo en realidad*, Paidós, 1999.

ICE
INFORMACIÓN COMERCIAL ESPAÑOLA

Información Comercial Española
Revista de Economía

6 números anuales

Artículos originales sobre un amplio espectro de temas tratados desde una óptica económica, con especial referencia a sus aspectos internacionales

Boletín Económico
de Información Comercial Española

12 números anuales

Artículos y documentos sobre economía Española, comunitaria e internacional, con especial énfasis en temas sectoriales y de comercio exterior

Acceso libre en
www.revitasice.com

INTERNET

Cuadernos Económicos
de ICE

2 números anuales

Artículos de economía teórica y aplicada y métodos cuantitativos, que contribuyen a la difusión y desarrollo de la investigación

www.revistasice.com
Teléfono 91 603.79.97/93
distribucionpublicaciones@mineco.es