POLÍTICA ANTES QUE REGULACIÓN: LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL EN LA ERA DEL *BIG DATA*

JOSÉ LUIS GÓMEZ-BARROSO (*)
Universidad Nacional de Educación a Distancia
CLAUDIO FEIJÓO
Tongji University –
Universidad Politécnica de Madrid
DOLORES F. MARTÍNEZ
Universidad de Murcia

Si algún tipo de información merece una especial atención por parte de los poderes públicos, es decir, el establecimiento de una política que considere cómo debe ser solicitada, tratada o transmitida, esa es sin duda la información personal, más aún cuando el análisis masivo de datos –el *Big Data*– promete ser uno de los ingredientes básicos de casi

cualquier negocio en casi cualquier sector económico de relevancia. Y, en efecto, atención ha recibido desde hace décadas. Hasta ahora, protección es la palabra que orienta, casi domina, las políticas que se ocupan de la información personal. La causa es simple: la información personal entra dentro del ámbito de lo privado al que el derecho siempre ha dado el máximo amparo. También por ello sería más preciso hablar de regulaciones que de políticas, pues el peso que en la actividad pública han tenido acciones diferentes de las estrictamente normativas ha sido muy reducido.

O al menos lo ha sido hasta ahora. Porque, reutilizando la estructura gramatical utilizada en el inicio, si algún tipo de política referida a información debe ser replanteada, esa es sin duda la política de protección de datos personales. En un escenario en que millones de datos personales son recogidos, tratados y utilizados con fines comerciales (o de otro tipo) y en que, lo que es aún más importante, muchas personas no perciben este hecho como algo realmente preocupante, sino incluso como un beneficio inmediato, los desajustes entre lo que pretende la norma y la realidad son más que evidentes.

Con ser urgente desde hace tiempo, el momento actual es particularmente oportuno para la reflexión acerca de cómo reorientar el uso y custodia de la información personal. Mientras en la Unión Europea se estaba alcanzando un acuerdo para la reforma de la reglamentación, el ambiente se enrarecía por la constatación de que, paradójicamente, los propios Estados (algunos Estados) pueden convertirse en la principal amenaza al derecho que deben defender. Y todo esto ocurre en un mundo crecientemente global e inmaterial, en que es prácticamente imposible poner puertas a los intercambios electrónicos de datos (también de los datos personales), y en que, por tanto, Europa tiene difícil hacer valer sus normas frente a las de otras regiones, en particular de aquellas en que esa economía digital que se alimenta de datos personales tiene su sede principal (léase Estados Unidos).

Considerando este contexto, y tras analizar cuál ha sido la evolución de las normas encargadas de la protección de datos personales, este artículo propone algunas líneas que, en opinión de los autores, deberían ser tenidas en cuenta en el diseño de las políticas que en el futuro se ocupen de la gestión de los datos perso-

nales. La estructura del artículo es la siguiente: en la primera sección se hace un repaso histórico de la política (legislación fundamentalmente) para la protección de la información personal y se considera la situación en Europa y en Estados Unidos; a continuación, se desgranan con algún detalle los factores que hacen necesario el cambio; el artículo se cierra con las propuestas para crear políticas ajustadas a este nuevo entorno.

LA EVOLUCIÓN DE LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL

Del derecho a la privacidad al derecho a la protección de datos personales

La privacidad, para la Real Academia el «ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión», siempre ha sido un valor digno de protección pública. Manifestaciones tempranas de esta protección pueden rastrearse en leyes de la Antigüedad clásica (Rebollo Delgado, 2005). Con las debidas adaptaciones sociales, culturales, e institucionales, la defensa tanto de la intimidad en la vida personal y familiar (Hafetz, 2002) como del secreto de las comunicaciones (véase el antiquísimo Belin, 1931) se mantuvo sin grandes cambios conceptuales hasta bien entrado el siglo XX. El repaso de la literatura académica indica que tras la segunda guerra mundial comenzaron a aparecer formas «modernas» de intrusión, tales como la apropiación de nombres o marcas o el acoso a los personajes públicos (Prosser, 1960), o también la revelación de historiales médicos (Coleman, 1961), pero sin que ello tuviera reflejo en los diversos ordenamientos jurídicos.

La noción legal se había ido consolidando en los primeros decenios del siglo XX, siempre con el contenido inicial, y así llegó a la Declaración Universal de Derechos Humanos (Naciones Unidas, 10 de diciembre de 1948), que en su artículo 12 recoge que «nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación». Similar es la redacción del artículo 8 de la Convención Europea de Derechos Humanos (Consejo de Europa, 4 de noviembre de 1950) y también la del artículo 12 del posterior Pacto Internacional de Derechos Civiles y Políticos (Naciones Unidas, 16 de diciembre de 1966).

Sin embargo, en el momento de la firma del Pacto, a mediados de la década de los sesenta, el entorno ya estaba alterándose. Era un cambio de entorno ante todo tecnológico. Las técnicas para el almacenamiento de información habían progresado y comenzaban a utilizarse con frecuencia por instituciones públicas y privadas. El uso que pudiera darse a estos almacenes de datos resultaba incierto. También se percibía como una amenaza la rápida mejora de aparatos como cámaras o micrófonos, básicamente por las opciones de vigilancia y espionaje que ofrecían. Avanzando por esta dirección, el trabajo precursor de Michael (1964) ya había aventurado que «[para 1984] compañías y gobiernos usarán los extraordinarios avances en la tecnología de computadores para recopilar y archivar hechos 'personales' [las comillas son de los autores] de los ciudadanos e incluso para telecontrolar la población», y algo más tarde Kalven (1967) definía un escenario prospectivo para final de siglo en que pronosticaba que todos viviríamos con un «imborrable registro de nuestro pasado y nuestras limitaciones» con lo que la sociedad habrá perdido «su benévola capacidad de olvidar». Conclusión clarividente.

Como efecto de todos estos avances, el fin de la década de los sesenta es también el momento en que se retoma la reflexión acerca de qué implica «lo privado». Una de las mejores constataciones de esa nueva inquietud la representa la obra de Alan Westin, quien en 1967 escribió que «pocos valores tan fundamentales para la sociedad como lo es la privacidad han sido dejados en tal estado de indefinición por la teoría social o han sido sujeto de tan vaga y confusa redacción por los científicos sociales» (Westin, 1967). Westin trató, además, de dar perfiles nuevos y más nítidos al concepto de privacidad que para él «es la reivindicación de personas, grupos o instituciones de poder determinar por sí mismos cuándo, cómo y con qué límites es comunicada a los demás información referida a ellos mismos». Pese a que Westin recoge, con razón, buena parte del reconocimiento, otros coetáneos habían también avanzado por caminos convergentes con el suyo (Bates, 1964; Jourard, 1966 o Gross, 1967).

La década de los setenta no vio progresos en lo jurídico, pero sí fue testigo de un salto cuantitativo en el registro computarizado de actividades y transacciones, en el uso de estrategias comerciales más próximas al cliente (lo que significaba que «se le conocía mejor») o en el número de litigios en que se denunciaba una invasión de la intimidad. Varios países establecieron comités con el encargo de estudiar el fenómeno; en algunas ocasiones, las conclusiones a que llegaron se incorporaron a normas (una descripción detallada se encuentra en OCDE, 2011). A la vez, el mundo académico seguía tratando de acotar definiciones y riesgos, cada vez más patentes (como ejemplo Breckenridge, 1970; Lusky, 1972; Goldstein y Nolan, 1975; Laufer y Wolfe, 1977). Y es que el volumen de datos que se guardaba no solo había crecido exponencialmente, sino que, más importante, había comenzado a moverse a una velocidad creciente. Por todo ello, la OCDE inició en 1978 el trabajo que culminó con la adopción de las «Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales» en septiembre de 1980. En las directrices se definen los datos personales como «cualquier información relacionada con un individuo identificado o identificable (sujeto de los datos)» y se dedica un apartado a una serie de principios básicos en el manejo de la información personal que aún hoy siguen siendo la base de prácticamente todos los ordenamientos: finalidad legítima (especificación del propósito), proporcionalidad (limitación de recogida y uso), necesidad de consentimiento, transparencia (derecho al acceso y a la rectificación), responsabilidad (deber de custodia), y restricciones a la transmisión.

Las dos últimas décadas del siglo XX están marcadas desde el punto de vista normativo por la consolidación y difusión de las directrices publicadas por la OCDE. La protección de los datos de carácter personal tomó cuerpo como derecho separado y distinto, aunque conectado, del respeto de la vida familiar y personal y de la protección de las comunicaciones. Esta diferenciación aparece en la mayor parte de las normas que se publicaron desde entonces. Valga por todas, la Carta de los Derechos Fundamentales de la Unión Europea, de marzo de 2000, cuyos artículos 7 y 8 tienen por título exactamente los conceptos que se acaban de citar. El primero de estos artículos sigue la línea tradicional y el segundo establece que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen, datos que «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».

Dejando los aspectos jurídicos y adoptando el punto de vista del entorno socioeconómico, en los últimos años del siglo XX se produjo un vertiginoso salto adelante en el aprovechamiento económico de la información personal. Este salto fue de la mano con la cotidianidad del uso de lo que ya para entonces se incluía bajo el término tecnologías de la información y de las comunicaciones. Pero si esas décadas fueron testigo de una auténtica convulsión en el uso de información personal, lo que ha traído la generalización del uso de internet ha sido un seísmo. En «la red», la colecta de datos es realizada en una escala de otra magnitud y de forma inmediata y mucho menos costosa. Por el solo hecho de comunicarnos y de acceder a o intercambiar información, dejamos trazas de quiénes somos, dónde estamos, qué hacemos o qué nos interesa, trazas que pueden ser (son de hecho) recogidas. Incluso se podría hablar de que existe un intento actual bastante generalizado para distinguir entre diversos tipos de información personal con el propósito, más o menos explícito, de separar algunos de estos datos y desligarlos lo más posible de la persona de tal forma que puedan ser aprovechados económicamente con menos restricciones o lo que es equivalente con un menor nivel de protección. Un ejemplo de uno de estos marcos de claro objetivo económico se puede encontrar en los trabajos del World Economic Forum (WEF, 2017), donde se distingue entre cuatro tipos de informaciones: i) la «identidad digital», conformada por las características que identifican unívocamente a una persona tales como nombre, edad, domicilio y similares; ii) la «personalidad digital», donde se reúnen los resultados del comportamiento en las diversas redes en las que el usuario participa como pueden ser las actualizaciones, reacciones u otras; iii) las «huellas digitales», constituidas por las trazas que el usuario deja cuando usa cualquier sistema digital, como pueden ser las *cookies* con datos de navegación o la localización procedente de una aplicación móvil; y iv) los «perfiles digitales», que son el resultado de combinar datos de un mismo proveedor o de varios y deducir con técnicas de análisis de datos masivos cuáles son los hábitos y preferencias de un usuario o de un colectivo de usuarios de medios y sistemas digitales.

Precisamente son todas las características de este nuevo entorno, de esta nueva economía de los datos masivos (Feijóo *et al*, 2016), donde confluyen y se confrontan diversos intereses –empresariales, de los consumidores, de los gobiernos- las que hacen apremiante una nueva (para el siglo XXI, para la era del *big data*) política sobre el uso de la información personal.

La regulación europea

Las directrices de la OCDE de 1980 son casi simultáneas con la «Convención para la protección de las personas en lo relativo al procesamiento automático de datos personales», que el Consejo de Europa acordó también a finales de 1980.

Quince años más tarde, el 24 de octubre de 1995, la ya entonces Unión Europea publicó la fundamental Directiva «relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos». Los datos personales son definidos con más detalle que en las directrices de la OCDE: «toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

En los años posteriores se confirió la máxima relevancia al derecho a la protección de los datos personales y se publicaron normas complementarias. La que podríamos denominar «constitucionalización» del derecho se inició en la ya citada Carta de Derechos Fundamentales de la Unión Europea del año 2000 en su artículo 8, continuó con su inclusión en el malogrado Tratado Constitucional de 2003, y se concretó finalmente en el articulado del Tratado de Funcionamiento de la Unión Europea (TFUE) en virtud del Tratado de Lisboa acordado en diciembre de 2007. El artículo 16 del TFUE establece que «toda persona tiene derecho a la protección de los datos personales que le conciernen».

En cuanto a las normas complementarias cabe citar el Reglamento 45/2001/CE, de 18 de diciembre de 2000, «relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos» y la Directiva 2002/58/CE, de 12 de julio de 2002, sobre la privacidad y las comunicaciones electrónicas. La Directiva de 2002 establece que los datos relativos a la localización y al tráfico deben borrarse o anonimizarse cuando dejen de ser necesarios para la comunicación o facturación (salvo en caso de consentimiento del abonado), y también que los Estados pueden limitar estas disposiciones para garantizar la seguridad nacional, la defensa o la seguridad pública siempre que ello «constituya

una medida necesaria, proporcionada y apropiada en una sociedad democrática». La Directiva fue modificada en 2006 y en 2009.

El 25 de enero de 2012 la Comisión publicó una propuesta de reglamento con la que pretendía modificar la Directiva 95/46/CE de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos. Dos días después se remitió tanto al Parlamento Europeo como al Consejo para informe. La dificultad para llegar a un texto de consenso se evidenció por el hecho de ser la propuesta legislativa que ha recibido mayor número de enmiendas, más de 3.000, en toda la historia del Parlamento. No fue hasta diciembre de 2015, ya con las nuevas instituciones surgidas tras las elecciones de 2014, cuando se alcanzó el acuerdo. El nuevo Reglamento 2016/679 del Parlamento Europeo y del Consejo, que mantiene el nombre de la ahora derogada Directiva de 1995 y se conoce con el sobrenombre de Reglamento general de protección de datos se publicó el 27 de abril de 2016. Junto a esta norma se publicó también una Directiva 2016/680 relativa «a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales».

La regulación de la información personal en Estados Unidos

Mientras que en la Unión Europea el uso de la información personal se regula de forma genérica y por tanto afecta a cualquier sector de actividad, en Estados Unidos no existe un marco normativo similar. En su lugar, existen una serie de regulaciones que se dirigen a sectores concretos de actividad.

El más regulado de todos los sectores es el público. Como resultado de la desconfianza generada a finales de la década de los años sesenta con respecto a las primeras bases de datos automatizadas, se publicó en 1966 la *Freedom of Information Act*, que concede el derecho de acceso a los datos recopilados por el gobierno federal, y en 1974 la *Privacy Act*, cuyo principal fin es controlar el uso sin autorización de los datos personales que las agencias federales recogen. Estas normas se han modernizado posteriormente, en particular en 1988, con la publicación de la *Computer Matching and Privacy Protection Act* y con la introducción de diferentes enmiendas con posterioridad a septiembre de 2002, enmiendas que ponen peso en el platillo de la seguridad en la balanza que forma con la privacidad.

Otros dos sectores que están sometidos a una regulación detallada son el sector financiero (*Fair Credit Reporting Act* de 1970) y el de la salud (*Health Insurance Portability and Accountability Act* de 1996). Por su parte, los proveedores de servicios de telecomunicación deben respetar las reglas establecidas en la *Electronic Communications Privacy Act* de 1986 y en la *Telephone Consumer Protection Act* de 1991.

En otros sectores, el comportamiento de las empresas con respecto al uso y almacenamiento de datos personales se rige por una combinación de obligaciones contractuales, estatutos generales y prácticas comunes de la industria que establecen lo que es «razonable» o «apropiado» (Gaff, Smedinghoff, y Sor, 2012), incluyendo una resistencia general a la existencia de regulación sobre datos de cualquier tipo (Hemerly, 2013). La autorregulación juega un papel importante en este esquema. Pero no existe una agencia que se encargue de la supervisión de sus resultados, lo que hace que las prácticas habituales sean, en general, mucho más laxas, que las que, como consecuencia del marco mucho más estricto, llevan a cabo las empresas europeas.

La regulación en otros países

Con excepciones (por ejemplo, Canadá aprobó en 2000 la *Personal Information Protection and Electronic Documents Act*) lo habitual en la mayoría de los países era que no existiera una única norma que regulara la protección de los datos personales. En algunos casos sigue siendo así (Australia), pero en muchos otros casos sí se han aprobado leyes específicas en los últimos diez años (Rusia y muchos países de Iberoamérica).

En el caso de China, sus ciudadanos no tienen reconocido ningún derecho individual con respecto a la intimidad. En los casos que llegan a los tribunales, los jueces suelen resolver haciendo uso del derecho a la «reputación», considerado un principio de derecho civil. Sin embargo, el gobierno chino estableció recientemente un grupo de trabajo para redactar una ley de protección de datos personales (Wu *et al.*, 2011). Más recientemente aún, en 2016, se ha aprobado una nueva ley de «ciberseguridad» que en teoría no permite que los agentes que recopilan información personal la ofrezcan a terceros sin consentimiento de los usuarios so pena de sanciones económicas.

En cualquier caso, cabe insistir en que las preferencias y percepciones sobre lo que son datos personales y hasta dónde cabe compartirlos es tremendamente variable. Cambia de usuario a usuario, cambia por edad, raza, sexo, nivel de estudios y nivel de ingresos. Y no menos diferente es la percepción entre geografías y países (KPMG, 2016).

UN NUEVO ESCENARIO PARA LA PRIVACIDAD

El entorno en que debe contextualizarse el concepto de privacidad está, desde hace medio siglo, en proceso de cambio. Cambio que se ha acelerado en los últimos tiempos debido a que las relaciones sociales y económicas están cada vez en mayor grado mediadas por relaciones computarizadas en las que la colecta de datos personales se realiza a gran escala y donde el atractivo de negocio del análisis masivo de datos no hace sino aumentar.

Las empresas recopilan datos para mejorar las técnicas de mercadotecnia con que comercializan sus productos. También para personalizar sus productos y servicios

y adaptarlos a las preferencias de los consumidores. Y no menos importante es aprender de los usuarios para innovar en la dirección que estos marcan. Pero quizá el modelo más obvio y directo ahora mismo es simplemente lograr que la audiencia a la que llega la publicidad de un cierto producto sea más ajustada a lo que busca el anunciante. Esta publicidad personalizada ha ganado importancia y de hecho está en la base del modelo de negocio de muchos de los gigantes de internet. Piénsese en los portales de entrada (de facto los buscadores) o las redes sociales más conocidas. De no mediar cambios radicales en el entorno, la evolución futura a medio plazo no hará sino acentuar todas las tendencias que ahora ya se pueden observar. El valor económico (difícilmente medible, pero con certeza creciente) de los datos personales (véase Gómez Barroso y Feijóo, 2013 para una aproximación general y Feijóo *et al*., 2014 para una aproximación cuantitativa) hace que las empresas busquen nuevas mañas para que los usuarios desvelen más y más información. Además, la expansión en el uso de dispositivos móviles genera opciones para un seguimiento, si cabe, más exacto (Feijóo *et al*., 2010).

Más importante aún, la manera en que los individuos perciben y gestionan la privacidad es ahora radicalmente distinta de la que era hace solo unos años. En ese sentido, como el fenómeno de las redes sociales claramente demuestra, existe una tendencia creciente hacia la compartición de detalles de la vida privada. Esto se combina con que el usuario (ciudadano) medio tiene un amplio desconocimiento de los procesos de recopilación de datos, de la profundidad de los rastros digitales que deja tras de sí, de los riesgos y de los medios para combatirlos. Cuando la cesión de datos es consciente, su comportamiento se rige por un conjunto de factores difícil de desentrañar, y con diferente peso en cada caso (Heirman *et al*., 2013; Taylor *et al*., 2015), entre los que está sin duda la percepción de lo que es socialmente aceptable (Trepte y Reinecke, 2013; Acquisti *et al*., 2012). Como consecuencia de los diferentes niveles de inquietud con respecto a la propia intimidad y el mayor o menor conocimiento de las posibles amenazas, la percepción del grado de intrusismo que generan las prácticas habituales de las empresas es variado (Schwaig, 2013; Bansal *et al*., 2015). Para complicar más este panorama, la llamada «paradoja de la privacidad» (puesta de manifiesto hace años en otros contextos y confirmada en la actividad en internet por numerosos estudios; véase un repaso en Kokolakis, 2017) indica que aquello que los individuos responden en las encuestas (lo que dicen que harían) no coincide con la realidad (lo que realmente hacen). Niveles de privacidad que *a priori* se declaran inadmisibles, son luego aceptados sin gran desasosiego en situaciones reales. Una situación más grave incluso para los jóvenes, que parecen haber aceptado un estado de cosas donde la privacidad en red se asume que es violentada casi por defecto (Hargittai, 2016).

Los «otros intereses de los Estados» son la siguiente pieza importante en el rompecabezas. Responsables de la protección del derecho, no debe olvidarse que las administraciones son el actor que más cantidad de datos almacena y que debe vigilar sus propias prácticas. Más importante aún es el conflicto entre privacidad y seguridad. Como algunas noticias recientes demuestran, los gobiernos pueden ser también invasores de la privacidad, la de sus propios ciudadanos o la de otros. Incluso si los fines sean considerados legítimos, ¿dónde está el límite para los controles «por razones de seguridad»?

Otra variable en la ecuación es el impulso de la economía digital. Todos los gobiernos ven en esta industria la vía para un desarrollo seguro y sostenible. Pero en una industria que ha acostumbrado al usuario a no pagar, o al menos a no hacerlo con dinero contante, la publicidad (y por tanto la recopilación de datos para poder realizar una publicidad más personalizada) es el principal camino alternativo (Feijóo y Gómez Barroso, 2013). Llegado el caso, ¿cambiaría la posición de Europa si las grandes empresas de internet tuvieran su sede a este lado del Atlántico?

Y por último también hay que considerar los «intereses de los otros Estados»: en un mundo global de intercambios inmateriales, en que los servicios pueden ofrecerse (se ofrecen) desde cualquier lugar del planeta, las normas «demasiado particulares» son difícilmente aplicables y fácilmente se quedan en mera intención.

REFLEXIONES FINALES: UNA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES PARA EL SIGLO XXI

El derecho a la privacidad se construye, en la práctica, preservando frente a injerencias externas unos ámbitos concretos de la esfera personal. El que cierta información sobre uno mismo no se difunda sin consentimiento es una de las intervenciones en que el derecho se concreta. Como parte de un derecho fundamental, que es el derecho a la intimidad, la protección de los datos personales se ha intentado asegurar con un entramado de normas imperativas. El fracaso que ha resultado de esta orientación es evidente a todas luces. Utilizando la mencionada terminología del WEF, perfiles digitales enormemente reveladores se construyen integrando datos disponibles para empresas y gobiernos –que los usuarios muchas veces desconocen que existen- y que se han obtenido por medios poco transparentes -cuando no opacos- a partir de las huellas, las personalidades y las identidades digitales de los usuarios y de aquellos con los que se relacionan.

Con ser importante el hecho de que los métodos legales existentes para la protección de datos personales no parezcan resultar válidos, más trascendente resulta el cambio en las convenciones sociales acerca de hasta dónde llega lo privado. Nuevas realidades requieren nuevas aproximaciones. Cuanto más complejas sean las realidades, más comprensivas deben ser las aproximaciones. Si quieren ser efectivas, las políticas de protección de la información personal deben convertirse en simples políticas de información personal. Políticas en que la protección siga formando el núcleo, pero en

que el catálogo de herramientas y de propuestas sea mucho más amplio. Incluso estas políticas podrían formar parte de un esquema más general denominado «gobernanza de los datos (del *big data*)» (véase Feijóo *et al*, 2016, para un planteamiento al respecto).

Obviamente la reforma del ordenamiento que se ocupa de la protección de datos personales es el primer paso. Esta reforma debe realizarse considerando la información personal, no solo como un derecho digno de protección, sino como un activo con valor económico. Guste o no, de no hacerse así, no estará atendiendo a lo que ocurre en la realidad y se estaría abocado a la ineficacia.

Pero para que unos usuarios ahora desinformados, e incluso indolentes respecto al tema, sean capaces de ejercer su derecho se necesita algo más que legislar. La educación de los usuarios de todo tipo de medios digitales es el primer elemento clave para que puedan decidir qué hacer con su privacidad.

A continuación, es necesario que la información que les llegue sea clara, lo que no es desde luego el caso ahora en que las políticas de privacidad de las compañías están escondidas y son complicadas de descifrar incluso para los no profanos, y en que las cláusulas sobre privacidad aparecen, minúsculas, enterradas al final de unos contratos de varias páginas.

Teniendo (y comprendiendo) información, el último aspecto es cómo hacer valer las decisiones. Herramientas que hacen posible que el usuario gestione, en buena medida, su privacidad, existen desde hace tiempo incrustadas en navegadores o en aplicaciones *ad hoc*. En realidad, lo que existe es toda una montaña de aplicaciones técnicas que conforman lo que se denomina «privacidad por diseño», cuyo fin es encastrar la privacidad de forma proactiva en la propia tecnología, haciendo que actúe por defecto (Camenisch, 2012 o Bélanger y Crossler, 2011, ofrecen recientes repasos del estado del arte). Pero, cuidado, un exceso de tecnología – de cifrado, por ejemplo- puede ocasionar una perdida de privacidad generalizada (Kamp, 2016, hace una brillante exposición al respecto), ya que la imposibilidad de acceder a información en ciertos supuestos supone un riesgo que diversos estados y jurisdicciones no están dispuestos a tolerar. Así que el progreso técnico es solo una parte, y contra la obsesión por las soluciones tecnológicas como la única otra alternativa frente a la legislación, ni siquiera la más importante. A su altura está la usabilidad y la simplificación de los procedimientos. Que el usuario no necesite habilidades o conocimientos inusuales para poder gestionar su privacidad es con total certeza una acción más eficaz para en conjunto darle poder al usuario que, por ejemplo, invertir en la mejora técnica de la propia herramienta de protección.

Un usuario consciente es un usuario capaz de elegir, o al menos de valorar, otras opciones, quizá más respetuosas con su privacidad. La pérdida del cliente es una amenaza sólida para que las empresas autorregulen sus actividades. En un mundo global, complejo y lleno de zonas grises, la vigilancia y la sanción son imprescindibles, pero probablemente insuficientes. Es también necesario impulsar acciones que a la postre supongan un incentivo para «la buena conducta». En este escenario de *big data,* la estricta regulación de la información personal debe dar paso a una auténtica política de información personal: el fin último no debe ser tanto la protección de los usuarios sino el dar a esos usuarios la opción (real) a estar protegidos.

(*) Nota de los autores: Este artículo forma parte de los trabajos para los proyectos: «Mobile Media & Personal Data: Comunicación móvil e información personal: impacto en la industria del contenido, el sistema publicitario y el comportamiento de los usuarios» del Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los retos de la Sociedad del Ministerio de Economía y Competitividad (CSO2013-47394-R); «Hacia un conocimiento de los mercados basados en el uso de información personal» del Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad. Ministerio de Economía y Competitividad (ECO2013-47055-R); y «Mob Ad: El impacto de la tecnología móvil en la comunicación estratégica y publicitaria» de la Fundación Séneca correspondiente a la Agencia de Ciencia y Tecnología de la Región de Murcia (19451/PI/14).

BIBLIOGRAFÍA

ACQUISTI, A.; JOHN, L.K.; LOEWENSTEIN, G. «The impact of relative standards on the propensity to disclose». *Journal of Marketing Research*, 2012, v. 49, n. 2, pp. 160-174.

BANSAL, G.; ZAHEDI, F.M.; GEFEN, D. «The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern». *European Journal of Information Systems*, 2015, v. 24, n. 6, pp. 624-644.

BATES, A.P. «Privacy – A useful concept?» *Social Forces*, 1964, v. 42, n. 4, pp. 429-434.

BÉLANGER, F.; CROSSLER, R.E. «Privacy in the digital age: a review of information privacy research in information systems». *MIS Quarterly*, 2011, v. 35, n. 4, pp. 1017-1042.

BELIN, E. «The privacy of telegraphic and radiotelegraphic transmissions». *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, 1931, v. 193, pp. 25-27.

BRECKENRIDGE, A.C. *The Right to Privacy*. Lincoln: University of Nebraska Press, 1970.

CAMENISCH, J. «Information privacy?». *Computer Networks*, 2012, v. 56, n. 18, pp. 3834-3848.

COLEMAN, A.H. «The patient's right to privacy». *Journal of the National Medical Association*, 1961, v. 53, n. 2, pp. 207.

FEIJÓO, C.; GÓMEZ-BARROSO, J.L., MARTÍNEZ-MARTÍNEZ, I.J. «Nuevas vías para la comunicación empresarial: publicidad en el móvil». *El Profesional de la Información*, 2010, v. 19, n. 2, pp. 140-148.

FEIJÓO, C., & GÓMEZ-BARROSO, J.-L. «Hacia una economía de la información personal». En J. M. Aguado, C. Feijóo, & I. J. Martínez (Eds.), *La comunicación móvil. Hacia un nuevo ecosistema digital* (pp. 305–321). 2013, Barcelona: Gedisa.

FEIJÓO, C., GÓMEZ-BARROSO, J.-L., & VOIGT, P. «Exploring

the economic value of personal information from firms' financial statements». *International Journal of Information Management*, 2014, v. 34, n. 2, pp. 248–256.

FEIJÓO, C., GOMEZ-BARROSO, J.-L., & AGGARWAL, S. «Economics of big data». In J. M. Bauer & M. Latzer (Eds.), *Economics of Internet*. 2016. Cheltenham: Edward Edgar Publishing.

GAFF, B.M.; SMEDINGHOFF, T.J.; Sor, S. «Privacy and data security». *Computer*, 2012, v. 45, n. 3, pp. 8-10.

GOLDSTEIN, R.C.; NOLAN, R.L. «Personal privacy versus corporate computer». *Harvard Business Review*, 1975, v. 53, n. 2, pp. 62-70.

GÓMEZ-BARROSO, J.L.; FEIJÓO, C. «Información personal: La nueva moneda de la economía digital». *El Profesional de la Información*, 2013, v. 22, n. 4, pp. 290-297.

HARGITTAI, E. «What Can I Really Do? Explaining the Privacy Paradox with Online Apathy». *International Journal of Communication*, 2016, vol. 10, pp. 3737–3757.

GROSS, H. «Concept of privacy». *New York University Law Review*, 1967, v. 42, n. 1, pp. 34-54.

HAFETZ, J.L. « *'A man's home is his castle?': Reflecti*Heirman, W.; Walrave, M.; Ponnet, K. 'Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior». *Cyberpsychology, Behavior and Social Networking*, 2013, v. 16, n. 2, pp. 81-87.

HEMERLY, J. «Public policy considerations for data-driven innovation». *Computer*, 2013, v. 46, n. 6, pp. 25–31.

JOURARD, S.M. «Some psychological aspects of privacy». *Law and Contemporary Problems*, 1966, v. 31, n. 2, pp. 307-318.

KALVEN, H. «Problems of privacy in year-2000». *Daedalus*, 1967, v. 96, n. 3, pp. 876-882.

KAMP, P.-H. «More encryption means less privacy». *Communications of the ACM*, 2016, v. 59, n. 4, pp. 40–42.

KOKOLAKIS, S. «Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon». *Computers, & Security*, 2017, n. 64, pp. 122-134.

KPMG. *Crossing the Line. Staying on the right side of privacy*. 2016. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/crossing-the-line.pdf

LAUFER, R.S.; WOLFE, M. «Privacy as a concept and a social issue – Multidimensional developmental theory». *Journal of Social Issues*, 1977, v. 33, n. 3, pp. 22-42.

LUSKY, L. «Invasion of privacy – Clarification of concepts». *Political Science Quarterly*, 1972, v. 87, n. 2, pp. 792-&.

MICHAEL, D.N. «Speculations on the relation of the computer to individual freedom and the right to privacy». *George Washington Law Review*, 1964, v. 33, n. 1, pp. 270-286´.

OCDE. *Thirty Years after the OECD Privacy Guidelines*. Organización para la Cooperación y el Desarrollo Económico, 2011. http://www.oecd.org/sti/ieconomy/49710223.pdf

PROSSER, W.L. «Privacy». *California Law Review*, 1960, v. 48, n. 3, pp. 383-423.

REBOLLO DELGADO, L. *El derecho fundamental a la intimidad*. Madrid: Dykinson, 2005.

SCHWAIG, K.S.; SEGARS, A.H.; GROVER, V.; FIEDLER, K.D. (2013). «A model of consumers' perceptions of the invasion of information privacy». *Information & Management*, v. 50, n. 1, pp. 1-12.

TAYLOR, J.F.; FERGUSON, J.; ELLEN, P.S. «From trait to state: Understanding privacy concerns». *Journal of Consumer Marketing*, 2015, v. 32, n. 2, pp. 99-112.

TREPTE, S.; REINECKE, L. «The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study». *Computers in Human Behavior*, 2013, v. 29, n. 3, pp. 1102-1112.

WEF. *Shaping the Future Implications of Digital Media for Society Valuing Personal Data and Rebuilding Trust End-User Perspectives on Digital Media Survey: Summary Report*. World Economic Forum, 2017. http://www3.weforum.org/docs/WEF_End_User_Perspective_on_Digital_Media_Survey_Summary_2017.pdf

WESTIN, A. *Privacy and Freedom*. Nueva York: Atheneum, 1967.

WU, Y.; LAU, T.; ATKIN, D.J.; LIN, C.A. «A comparative study of online privacy regulations in the U.S. and China». *Telecommunications Policy*, 2011, v. 35, n. 7, pp. 603-616.