Papeles el tiempo de los derechos

NUEVAS TECNOLOGÍAS, BIG DATA Y DERECHO AL OLVIDO DIGITAL: ¿SUPONE EL NUEVO REGLAMENTO EUROPEO DE DATOS PERSONALES UN CAMBIO DE MODELO?

Marina Sancho López
Investigadora contratada en formación en la Universitat de València,
Departament de Dret Civil.
marina.sancho@uv.es

Palabras clave: Derecho y nuevas tecnologías, Big Data, Derecho al olvido, Protección de datos, Privacidad, Internet.

Número: 7 Año: 2018

ISSN: 1989-8797

Comité Evaluador de los Working Papers “El Tiempo de los Derechos”

María José Añón (Universidad de Valencia)
María del Carmen Barranco (Universidad Carlos III)
María José Bernuz (Universidad de Zaragoza)
Manuel Calvo García (Universidad de Zaragoza)
Rafael de Asís (Universidad Carlos III)
Eusebio Fernández (Universidad Carlos III)
Andrés García Inda (Universidad de Zaragoza)
Cristina García Pascual (Universidad de Valencia)
Isabel Garrido (Universidad de Alcalá)
María José González Ordovás (Universidad de Zaragoza)
Jesús Ignacio Martínez García (Universidad of Cantabria)
Antonio E Pérez Luño (Universidad de Sevilla)
Miguel Revenga (Universidad de Cádiz)
Maria Eugenia Rodríguez Palop (Universidad Carlos III)
Eduardo Ruiz Vieytez (Universidad de Deusto)
Jaume Saura (Instituto de Derechos Humanos de Cataluña)

Nuevas tecnologías, Big Data y Derecho al olvido digital: ¿Supone el Nuevo Reglamento Europeo de Datos Personales un cambio de modelo?

Marina Sancho López
Investigadora contratada en formación en la Universitat de València,
Departament de Dret Civil.
marina.sancho@uv.es

I. Introducción

> *Las instantáneas fotográficas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: «lo que le susurre en la intimidad será proclamado a los cuatro vientos».*
> (Samuel Warren y Louis Brandeis, *Right to Privacy*)

Famoso es el artículo que en 1890 Warren y Brandeis escribieron en el *Harvard Law Review*[1] y que, haciendo crítica de las prácticas amarillistas de algunos periódicos de la época, revolucionó el concepto de la intimidad personal en el ámbito jurídico.
El texto, célebre por su construcción jurídica de la privacidad sobre la base del derecho de propiedad, reivindicaba el "*right to be let alone*" (derecho a no ser molestado) con unas reflexiones aún de plena actualidad pese a sus más de cien años de historia.

Si las instantáneas fotográficas junto con los emergentes métodos periodísticos y su incidencia en la esfera privada de las personas fueron lo que llevaron a estos abogados bostonianos a decir basta y a escribir un artículo en defensa de nuevos métodos de protección jurídica frente a tales intromisiones, cuesta imaginar qué dirían de la situación actual en la que prácticamente todos tenemos un Smartphone con conexión a Internet con el que nos exponemos y estamos expuestos en términos de privacidad.

[1] WARREN, S., BRANDEIS, L. *The right to privacy*, Harvard Law Review, 1890, p. 195.

Los avances científicos y los cambios tecnológicos que los impulsan constituyen la paradoja del siglo XXI, haciéndonos libres al mismo tiempo que hipotecan nuestra vida privada, creando constantemente nuevos peligros para la intimidad, infinitamente más sitiada hoy que en la época de Warren y Brandeis.

Nadie ha resultado ajeno a este nuevo escenario y, con él, hemos cambiado por completo nuestra forma de relacionarnos, los hábitos culturales y hasta nuestras pautas de comportamiento.
Que Internet y las nuevas herramientas informáticas han logrado acercar a los ciudadanos de todo el Mundo y que han traído aparejadas numerosas ventajas son hechos incuestionables. Sin embargo, esto también tiene un reverso y es que con ello se ha modificado, para mal, la configuración tradicional de la privacidad.

El ámbito de la intimidad es el último reducto de la personalidad, un espacio en el que el individuo es el único soberano. La intimidad, tal y como se ha consolidado en la doctrina, incluye también el derecho a controlar la información sobre uno mismo, a la llamada autodeterminación informativa. Sin embargo, las vigentes prácticas empresariales llevadas a cabo por las operadoras de Internet, han supuesto un incremento sin precedentes del intercambio (acceso, almacenamiento, tratamiento y uso electrónico) de datos personales a gran escala, suponiendo una amenaza para los principios fundamentales sobre los que se asienta el derecho a la protección de datos personales y, en especial, el derecho a la intimidad, por lo que parece necesario reafirmar su contenido y reivindicar su protección.

Ante un panorama evidente de pérdida de privacidad, los Estados han legislado tratando de dar una mayor cobertura a las garantías personales protegidas por los derechos tradicionales, cuyos mecanismos de protección se han revelado obsoletos ante una realidad tecnológica en constante renovación.
Sin embargo no podemos resignarnos y considerar la privacidad como una utopía, la sociedad globalizada y tecnológica actual debe poder dar respuestas jurídicas ante los desafíos que se presentan, adaptándose a la nueva realidad digital.

II. Nuevas tecnologías y protección de datos, ¿realidades antagónicas?

Podemos afirmar sin temor a equivocarnos que nos encontramos ante una expropiación sin precedentes de la privacidad.

El acceso masivo de la sociedad a Internet ha devenido una auténtica revolución cultural, que no ha quedado en una apertura de puertas a la información y la comunicación sino que ha ido más allá, alterando por completo hábitos sociales, de consumo y hasta patrones de comportamiento.

En este contexto, los fenómenos tecnológicos de los últimos tiempos han originado nuevos escenarios dónde la vulnerabilidad de nuestros datos personales es más que evidente.

Nuestra forma de entender la vida ha cambiado por completo, ya no es tan significativo, ni tan siquiera fácil, distinguir entre lo *offline* y lo *online* pues hoy en día todo tiende a estar conectado y dichas barreras se diluyen constantemente (un ejemplo sencillo lo encontramos cuando realizamos una compra por Internet pero procedemos a su devolución en una tienda "física"). La interacción de las personas en el ciberespacio es real y forma parte de la cotidianeidad, pasando éste a convertirse en una prolongación de la sociedad "física", con más virtudes si cabe pero con aún más defectos, al menos, para la protección de muchos de nuestros derechos.

Y es que este marco se traduce en una concentración de datos personales a gran escala a través de nuevas vías para su captura, indexación y procesamiento. Por lo que, sin desmerecer las innumerables ventajas que vienen aparejadas al acceso a las más recientes tecnologías, es innegable el potencial lesivo para derechos como la intimidad, que acarrean[2].

Las nuevas tecnologías "inteligentes" funcionan a partir de datos y metadatos –los metadatos son datos sobre los propios datos, además de qué y quién, dan respuesta al cuándo, cómo, dónde… permitiendo crear catálogos de ficheros de datos con el objetivo

[2] Cuanto más extensa es la innovación tecnológica y cuanto mayor es su generalización, menor es el ámbito de privacidad reservado a los individuos, lo que se traduce consecuentemente en un potencial riesgo para la libertad y la igualdad, en lo que PÉREZ LUÑO ha denominado "asalto tecnológico de los derechos y libertades". PÉREZ LUÑO, ANTONIO. Los derechos humanos en la sociedad tecnológica, Madrid, Universitas, 2012, p. 23.

de explotarlos posteriormente, por ejemplo, para fines publicitarios[3]- que les proporciona el propio usuario y que, junto con otros parámetros, permiten configurar un patrón personal capaz incluso de predecir el comportamiento. Es por ello que nuestro *smartphone* nos recuerda que próximamente tenemos cita con tal médico, nos sugiere una ruta alternativa para llegar a casa según las condiciones de tráfico, nos avisa de que el próximo mes tenemos un congreso en Barcelona y hasta se toma la libertad de indicar que nuestra calidad del sueño no ha sido óptima[4].

Estos datos y metadatos se consiguen, generalmente, a través de las aplicaciones que descargamos en nuestros dispositivos inteligentes que cada vez con más frecuencia exigen para poder instalarlas acceso a información personal de lo más dispar, como la agenda de contactos, las fotografías, la ubicación en tiempo real, el calendario… en la casi totalidad de casos, sin que sea necesario para el funcionamiento de la aplicación en concreto.

La instalación de estas aplicaciones supone auténticos contratos de adhesión dónde los usuarios sólo tenemos la facultad de decidir si instalamos –con todas las condiciones- o no la misma, pero sin ningún poder de transacción al respecto de sus cláusulas. Y, a través de estos programas, se produce el acceso y exportación de datos y metadatos que, no en pocas ocasiones, sucede sin autorización expresa o sin conocimiento del propio usuario.

No se niega la ayuda que nos proporcionan cuotidianamente estos datos, indicando cuánto queda para llegar a casa o cuál es el mejor camino para evitar un atasco, ni tampoco que estas cuestiones, por el momento, no sean de gran preocupación para el conjunto de los ciudadanos, sin embargo, no puede ignorarse el hecho de que se está vulnerando nuestra intimidad constantemente, muchas veces sin tener conocimiento de ello, y desconociendo el alcance de sus consecuencias.

---

[3] Así, si un teléfono móvil tradicional tenía información sobre las llamadas y mensajes efectuados, un Smartphone es capaz de almacenar infinidad de datos acerca de nosotros: cuántas calorías consumimos de media, cuánto tiempo dormimos, cuánto dinero solemos gastar en el supermercado, qué tipo de prensa leemos habitualmente y en qué noticias estamos más interesados… hasta el punto de poder hacerse una configuración del usuario en base a sus patrones de comportamiento que, aunque muchas veces diste de la realidad, permite clasificar a los usuarios según su supuesto nivel adquisitivo o sus intereses culturales, por ejemplo.

[4] HILDEBRANDT, MIREILLE. *Slaves to Big Data. Or are we?*, Revista de los Estudios de Derecho y Ciencia Política, n.17, 2013. La autora, para definir los metadatos, se ayuda de una analogía con el sistema nervioso del cuerpo humano que, de manera autónoma, dirige nuestro entorno interno, de una forma a la que no tenemos acceso consciente y sobre la que no tenemos control directo.

Un ejemplo lo tenemos en los nuevos contadores inteligentes de luz instalados por la compañía eléctrica de forma obligatoria para sus usuarios –por el que pagamos un alquiler mensual, por cierto- que procesan nuestros datos de consumo en tiempo real. Los datos que extraen se combinan con unos precios flexibles que son distintos cada día, cada hora y para cada cliente de una forma sobre la que los usuarios no tenemos control directo pero que, sin duda la compañía eléctrica le está sacando rédito. Teniendo en cuenta los datos sobre el consumo real de luz de los usuarios, la compañía eléctrica puede hacer estimaciones de consumo en base a predicciones sobre los patrones de comportamiento de sus usuarios, rentabilizando esta información en forma de operaciones de mercado. Es decir, frecuentemente se monetizan dichos macrodatos por las empresas privadas.

Otra cuestión directamente relacionada con lo que se viene tratando es la actual capacidad de condicionamiento e, indirectamente control, que ostentan las corporaciones de Internet y los operadores de telecomunicaciones respecto de sus usuarios, y que en la práctica supone una supresión progresiva (pero masiva) de la privacidad por medio de la entrega de servicios falsamente gratuitos que imponen unilateralmente cláusulas abusivas respecto de los datos personales de sus usuarios, a los que someten a una vigilancia constante.

Los contratos de adhesión que imponen la instalación de las aplicaciones que exigen las nuevas tecnologías contienen, en su mayoría, cláusulas abusivas sobre las que el usuario no tiene ningún poder de negociación. Y aún resulta más abusivo el cambio unilateral de las políticas de privacidad (bajo el eufemismo “condiciones o términos de uso”) de aplicaciones o programas que el usuario ya tiene instalados en su dispositivo, y que buscan obtener un mayor grado de datos personales, con la proporcional y consecuente disminución de la privacidad que conlleva.

Si bien es cierto que se informa al usuario de los cambios al respecto, ¿cuántos de nosotros hemos leído las 30 páginas de las que constan los usos y términos del servicio antes de instalar la aplicación WhatsApp? Y, de haberlo hecho, no puedo afirmar con seguridad que hubiésemos entendido el 100% de su redacción.

Así, por una parte las empresas están obligadas a detallar de forma comprensible su política empresarial y nosotros a leerla detenidamente, aunque sin embargo partimos de premisas totalmente falsas; por otra parte, es innegable que al usuario le resulta mucho más fácil tolerar cambios en las condiciones de uso de aplicaciones que usa diariamente que aceptarlas por primera vez en caso de ser un nuevo cliente[5].

Un ejemplo muy clarificador lo encontramos en WhatsApp, el servicio más conocido de mensajería instantánea (concebido así en su nacimiento aunque, en la actualidad, es mucho más que eso ya que permite hacer llamadas de voz y video o enviar fotos e hipervínculos) a través de dispositivos inteligentes y en principio gratuito, motivo por el que se ha generalizado su uso. WhatsApp, en agosto de 2016, actualizó sus "términos de servicio" y su "política de privacidad" de manera unilateral para conseguir compartir con Facebook (que en 2014 compró la empresa WhatsApp) y todo su grupo empresarial, los datos de los usuarios de la primera.
Aunque, la actualización automática de estas condiciones contractuales eliminaba por defecto, y de forma paradójica, toda privacidad de sus usuarios, se permitió a éstos oponerse a algunas pequeñas estipulaciones, sin demasiadas transigencias relevantes (los nuevos clientes ni siquiera tendrían esta opción).

Entre los datos que a partir de entonces se transfieren a Facebook y otras empresas asociadas encontramos: los números de la agenda de contactos del dispositivo (incluso de aquellos que no son clientes de WhatsApp), el nombre, estado y foto de perfil de cada usuario, su geolocalización, horarios y rutinas de conexión e, incluso, información sobre la transacción de cuentas bancarias (para aquéllos que hayan pagado WhatsApp). Además, con ello también se autoriza a transferir datos a las Autoridades que así lo soliciten, sin obligación alguna de comunicárselo a los afectados[6].
Es decir, las nuevas cláusulas contractuales de WhatsApp permiten extraer infinidad de metadatos capaces de establecer patrones de comportamiento prácticamente unívocos -teniendo en cuenta que hoy en día llevamos el móvil prácticamente a todos lados-, cómo

[5] Una operación de marketing de sobra conocida y que, además, es plenamente efectiva, es ofrecer servicios de forma gratuita durante un tiempo de prueba después del cual el usuario, ya acostumbrado a su uso, deberá decidir si contratarlos y seguir disfrutando de ellos o, por el contrario, prescindir de éstos.
[6] Resulta sorprendente que, al mismo tiempo que WhatsApp implantaba dichas modificaciones, eludía explícitamente la responsabilidad total en caso de ocurrir algún incidente de seguridad capaz de robar los datos personales de sus usuarios. En palabras textuales, WhatsApp no garantiza que nuestros datos estén "protegidos ni seguros".

cuándo y a qué red wifi nos conectamos o cuáles son los comercios en los que solemos comprar.

No hay duda de que los datos personales resultan sumamente valiosos para este tipo de empresas, que mediante la implantación de nuevas tecnologías intentan aumentar en lo posible su volumen, lo que, consecuentemente implica una vigilancia comercial de civiles[7] aparejada a una pérdida proporcional de la privacidad.
El Nuevo Reglamento Europeo de Protección de Datos intenta resolver algunas de estas cuestiones, al menos armonizando las legislaciones domésticas y evitando la fuga de las empresas operadoras de Internet y responsables de dichos comportamientos, y habrá que estar atentos a su aplicación y operatividad en esta materia.

i. La privacidad: el petróleo del siglo XXI

En la sociedad globalizada actual, las innovaciones tecnológicas junto con el nuevo modelo económico y social, han hecho proliferar enormes cantidades de bases de datos de carácter personal. Éstas, se convierten mediante algoritmos en información digital que resulta indudablemente valiosa en términos empresariales y económicos para las empresas que operan en Internet.

El denominado Big Data se ha convertido en una herramienta empresarial imprescindible dada su capacidad para influir en los hábitos de consumo de la economía actual. La Sociedad de la Información está poniendo la tecnología más avanzada al servicio de los desafíos comerciales tradicionales, provocando con ello una transformación del sistema de consumo y del empleo de las estrategias publicitarias, al mismo tiempo que está generando nuevas amenazas y desafíos en materia de privacidad.

Este proceder supone la acumulación de información en enormes bancos de datos, relativos a la identidad (nombre, profesión, lugar de residencia, estado civil, propiedades…) u otra información personal tan diversa como la religión, ideología,

[7] DEL FRESNO GARCÍA, MIGUEL. *Haciendo visible lo invisible: visualización de la estructura de las relaciones en red en Twitter por medio del análisis de redes sociales*, El profesional de la información, n.3, 2014.

clase social, salud… La información, en el primer caso, se obtiene de registros públicos o privados y por ello podríamos decir que es "real" mientras que, en el segundo caso, se trata de información obtenida a través de otros parámetros -no siempre fiables- como por ejemplo, pautas de comportamiento, preferencias culturales o patrones de consumo.

Ambos tipos de información quedan almacenadas en enormes bases de datos y unos y otros permiten identificarnos o reconstruir nuestra identidad. Este proceso, llevado a cabo masivamente por parte de las empresas de telecomunicaciones, sumado a los datos generados por las Administraciones públicas y las industrias privadas de seguridad, es lo que se ha denominado por algunos autores como *Dataveillance,* o dicho de otra forma: la normalización social de la cultura de la vigilancia[8].

Por poner un ejemplo, empresas como Google o Facebook no son una excepción en el contexto capitalista actual dónde la motivación empresarial se rige por criterios económicos. No hay que confundir el hecho de que estén ofreciendo servicios sin coste económico para sus usuarios con la filantropía o con motivaciones ajenas a la lógica del beneficio, lo que ocurre es que su provecho no reside en las cuotas o precios de sus usuarios sino que proviene, indirectamente, de los datos personales de éstos.

El negocio es más que rentable: a cambio de la instalación de una App, mediante la suscripción a un boletín de noticias o permitiendo la geolocalización del Smartphone, los usuarios ceden de forma totalmente gratuita sus datos y metadatos personales a empresas que los almacenan o los venden a terceros, y los procesan para un tratamiento posterior con fines, por ejemplo, de publicidad.
Así, los usuarios de estos servicios ya no somos simples consumidores pasivos sino que, con esta expropiación de nuestra privacidad, somos parte del producto cuya ganancia, dista de recaer en nosotros.

Pero no sólo se trata de acumular datos, sino de interrelacionarlos entre sí para lograr aumentar exponencialmente la información a obtener y sacarle así un mayor partido. Es

[8] Lo que FROSINI denominó "juicio universal permanente" hace más de treinta años y al que algunos acusaron de conspiracionista, hoy en día y teniendo en cuenta la monitorización electrónica de nuestro día a día, vuelve a estar de plena actualidad. FROSINI, VITTORIO. Cibernetica, Diritto e Società, di Comunità, 1978.

lo que SOLOVE[9] llama *agregación*: conformar el perfil de una persona a través de la triangulación y organización de la información que se ha obtenido sobre ella, obteniendo de este modo nuevos datos sobre un mismo individuo.

La expropiación sin precedentes de la privacidad en la que nos encontramos no es casual, tiene sus motivos. Y es que la privacidad tiene claramente un valor de mercado, además en alza, y se ha convertido en la nueva moneda del mercado online, pasando del Internet de las cosas al Internet de las corporaciones donde las cosas somos nosotros y en el que los datos personales son el producto a comercializar[10].

Este fenómeno se magnifica con las redes sociales que se están convirtiendo, en la práctica, en un software de gestión de datos personales que, para más provecho de las corporaciones que operan en el campo del Big Data, están directamente proporcionados por los usuarios que son precisamente quienes nutren de contenido las mismas: con comentarios, fotografías, ubicaciones geográficas, preferencias ideológicas y de consumo… un conglomerado de información que posteriormente se mercantiliza por los propietarios de las redes sociales, cediendo o vendiendo información a terceros o almacenándola para su tratamiento posterior.

Para una mayor comprensión tomemos como ejemplo la red social Facebook, que ofrece un servicio sin coste económico para sus usuarios al mismo tiempo que se constituye en una entidad empresarial con todas las letras, que cotiza en bolsa y cuya finalidad es tan simple como legítima: obtener beneficios económicos.

Mientras que sus ingresos los proporciona la publicidad, su activo empresarial está formado por la gran cantidad de datos y metadatos que almacena en su sistema, lo que explica que Facebook tenga un valor de mercado muy superior a sus ganancias y también que haya llevado a cabo operaciones empresariales como la compra de

[9] SOLOVE, D.J., *A Taxonomy of Privacy*, University of Pennsylvania Law Review, Vol. 154, núm. 13, 2006.
[10] DEL FRESNO GARCÍA, MIGUEL. *Internet como macromedio: la cohabitación entre medios sociales y medios profesionales*, Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad, n.99, 2014.

WhatsApp[11] o de Instagram, con el propósito de aumentar la gran cantidad de información personal que atesora.

Resulta paradójico que las redes sociales, como fenómeno social fruto de la revolución tecnológica de los últimos tiempos, frecuentemente se describan como un altavoz de la libertad de expresión y la información cuando, al mismo tiempo, conllevan consecuencias perjudiciales para la intimidad de sus usuarios, que son tratados como mercancía para la obtención de sus propios beneficios empresariales. No resulta disparatado concluir que la libertad y la privacidad, son grandes damnificadas de las nuevas tecnologías.

Sin embargo, esto es sólo la punta del iceberg, porque más allá de las evidentes connotaciones negativas que arrojan para la privacidad de los ciudadanos, el problema del almacenamiento masivo de datos personales está aún por determinar.

Pues si bien en la actualidad la información extraída se emplea para fines publicitarios, desconocemos qué finalidades y aplicaciones futuras tendrá. Si bien se ha demostrado que las empresas que operan en el marco del Big Data tienen como objetivo último la consecución de beneficios económicos, no es descabellado pensar con qué propósitos futuros emplearan toda la información personal que ahora están atesorando y hasta qué punto estarán dispuestas a comercializar con ella.
Es decir ¿qué ocurriría si una empresa como Facebook decide ofrecer los datos personales de sus usuarios, por ejemplo, a una compañía de seguros? O peor aún, ¿Qué ocurriría si esta información cae en manos de la economía criminal? Los expertos advierten que el tráfico ilegal de metainformación se presenta como un negocio en auge[12].

Así las cosas, podemos afirmar que los datos personales son el petróleo del siglo presente, pues ellos orientan el desarrollo y uso de nuevos productos y servicios. Y

[11] Puede ayudar a hacerse una idea de cuánto valor tienen los datos personales la astronómica cantidad de 21.800 millones de dólares que Facebook pagó por la compra de WhatsApp en 2014, un volumen desproporcionado teniendo en cuenta los precedentes en la industria.
[12] En el mercado negro, por ejemplo, un historial clínico tiene actualmente más valor que una tarjeta de crédito. Cada vez son más frecuentes las noticias en torno al robo de los datos personales como, por ejemplo, el secuestro de datos personales sanitarios. http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030?maca=en-rss-en-all-1573-rdf

resulta que la obtención de información personal cuenta con dos grandes aliados, de una parte las nuevas herramientas tecnológicas y, de otra, la fragmentación legislativa o incluso la desregulación, por lo que en la actualidad se está efectuando un mercadeo de datos personales sin demasiados problemas.
Estos dos factores contribuyen a la mercantilización de la privacidad de los ciudadanos, como el producto estrella a comercializar por las grandes corporaciones del Big data, y veremos si el Nuevo Reglamento Europeo de Protección de Datos puede poner o no coto a esta situación.

ii. Breve descripción de la situación jurídica actual

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) regula el registro, el tratamiento y toda modalidad de uso posterior de esos datos por los agentes públicos y por empresas privadas y para ello articula algunos principios de actuación así como una serie de mecanismos que permiten a los ciudadanos ejercer sus derechos, por ejemplo, de acceso, rectificación y cancelación de su información personal contenida en algunos de estos ficheros. La LOPD, como no podía ser de otra manera, se basa en el consentimiento que el afectado por el tratamiento de dichos datos debe prestar en todo momento, así como en la información clara y detallada que previamente debe recibir para consentir.
Sin embargo, ¿cuántos usuarios leen atentamente los usos y términos del servicio antes de instalar una aplicación? Y, en caso de hacerlo, ¿cuántos de ellos entienden efectivamente todos los pormenores? La LOPD obliga a las empresas a detallar de forma comprensible su política de privacidad y el usuario tiene la obligación de leerla, aunque estos dos extremos no se cumplan con demasiada frecuencia.

El oscurantismo con que se llevan a cabo estas prácticas empresariales es palmaria y flagrante como también lo son las cláusulas abusivas de contratación y ni qué decir tiene la modificación unilateral de las mismas. Pero además de las cláusulas ambiguas nos encontramos ante un problema de jurisdicción y es que, a pesar de operar en nuestro país, la mayoría de proveedores de servicios de Internet se encuentran en suelo americano, un "paraíso de privacidad" cuya legislación ampara la mercantilización de los datos personales, lo que ha supuesto en la practica un éxodo masivo de estas

empresas hacia la jurisdicción estadounidense[13], que acoge éstas y otras prácticas empresariales de dudosa legalidad en suelo europeo.

Conviene recordar aquí, lo acontecido con el *Safe Harbor* y la Sentencia del TJUE de 2015 en el caso Schrems[14] que lo declaró inválido.

La regulación europea en materia de protección de datos anterior al vigente Reglamento, prohibió la transferencia internacional de datos personales de ciudadanos europeos a países que no contasen con ciertos estándares de protección, entre ellos, Estados Unidos. ¿Entonces cómo operan empresas como Facebook?

Para lograr el intercambio comercial de datos entre la Unión Europea y los Estados Unidos entró en vigor el año 2000 el *Safe Harbor* (Puerto Seguro), una norma de adhesión voluntaria a la que se suscribieron empresas que operaban con datos a los dos lados del atlántico para garantizar así el tráfico de los mismo, a cambio de acatar el cumplimiento de ciertas normas de seguridad[15].

A raíz de las filtraciones llevadas a cabo en 2013 por Edward Snowden, excontratista de la NSA y la CIA, se dejaron en evidencia las prácticas de espionaje masivo que se estaban llevando cabo por agencias de EEUU -en colaboración con otros países aliados- sobre la población mundial[16]. Esto llevó al TJUE, a raíz de una demanda presentada por un ciudadano austríaco que arremetía contra Facebook por vulnerar su privacidad, a concluir que Estados Unidos no era un país seguro en materia de privacidad, abriendo la puerta a los Estados europeos a que declarasen, si así lo estimaban, que el tratamiento de datos de sus ciudadanos por EEUU era ilegal.

Sin embargo esto no significó el fin de las transferencias de datos personales desde la UE hasta los EEUU pues, aunque el nuevo Reglamento Europeo de Protección de Datos

[13] Un ejemplo de ello lo encontramos en la polémica inauguración en el año 2014 del centro de datos más grande del Mundo (equivalente a quince estadios de fútbol) a manos de la Agencia de Seguridad Nacional de EEUU para el análisis de los mismos. http://www.bbc.com/mundo/noticias/2012/03/120326_mayor_centro_espias_eeuu_fp.shtml?print=1.

[14] Sentencia de 16 de octubre de 2015, asunto C-362/14, disponible en http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=105220.

[15] Los requisitos que se exigían para formar parte del *Safe Harbor* eran de muy fácil cumplimiento, mucho menos rígidos que los exigidos por la normativa europea en protección de datos, por lo que casi cualquier empresa estadounidense que lo solicitase entraba a formar parte de él. Se puede consultar la lista completa en: https://safeharbor.export.gov/list.aspx.

[16] http://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm.

endurece los estándares de seguridad, por otro lado, Estados Unidos y la Unión Europea ya han llegado a un nuevo acuerdo llamado *Privacy Shield* (Escudo de Privacidad) que, aunque impone mayores exigencias a las compañías estadounidenses, les permite de facto, seguir mercadeando con los datos personales de los ciudadanos europeos con total impunidad.
En definitiva, la transferencia internacional de datos se está convirtiendo en la regla general y no en la excepción.

III. El derecho al olvido en el contexto del Big Data

Como ya se ha dicho, el auge tecnológico en el campo de Internet ha venido aparejado, junto a evidentes ventajas, de nuevas amenazas para algunos derechos fundamentales. Un ejemplo lo encontramos en los motores de búsqueda online como Google que, al facilitar el acceso masivo a la información así como su almacenamiento, conservación y difusión, vulnera en ocasiones el honor o la intimidad de las personas.

Frente a este nuevo escenario, conceptos jurídicos como *intimidad* o *vida privada* han cobrado un nuevo significado y los mecanismos tradicionales para su protección se han descubierto ineficaces, lo que ha motivado el desarrollo de nuevas construcciones jurídicas capaces de reforzar el control sobre nuestros datos personales.

La gestación del derecho al olvido obedece a la necesidad de proteger la privacidad frente a las nuevas amenazas generadas por las modernas herramientas informáticas. Pretende ser un nuevo mecanismo de protección concediendo a los usuarios de Internet la posibilidad de suprimir los datos personales (como imágenes, textos, opiniones, documentos oficiales, certificados o cualquier otro que describa un comportamiento u acción pasada) de la lista de resultados servida por los motores de búsqueda o publicados en sitios web, redes sociales, blogs, etc.

Las nuevas tecnologías han supuesto la digitalización masiva de la información así como su almacenamiento por defecto que se erige como regla general, se ha vuelto menos costoso que eliminarlos o hacerlos anónimos, por lo que ejercer los derechos de rectificación, oposición y cancelación de los datos personales parece ir en contra de la

tendencia natural de la economía. Este escenario no puede pasar inadvertido de ningún modo para el Derecho, que ha de adaptarse para conseguir una eficacia real en la protección de los derechos de los ciudadanos. Los prestadores de contenidos y servicios de Internet deben asumir la responsabilidad que de sus actuaciones corporativas se derive para los derechos humanos, y conceder a los usuarios la posibilidad de reclamar su cumplimiento.

El derecho a olvido aspira a ser la respuesta jurídica al problema obligando, por ley, a borrar o hacer anónimos los datos personales una vez se haya logrado el objetivo de su tratamiento, concediendo al titular el derecho a oponerse justificadamente al mismo. Se pretende impedir así el perpetuo mantenimiento de algunos datos en Internet altamente sensibles para la dignidad e intimidad de las personas como, por ejemplo, la eliminación o bloqueo de datos de ficheros de morosos o de listados comerciales, o la cancelación de antecedentes penales.

A pesar de que el derecho al olvido es un concepto reciente aún sin consolidar en nuestra tradición jurídica[17], sí lo es el derecho a la protección de datos, a la intimidad, al honor y a la dignidad, contemplados en la práctica totalidad de legislaciones nacionales vecinas y en el marco europeo. Por ello, ante una situación en la que los mecanismos jurídicos tradicionales se revelaban como ineficaces, la evolución lógica que se le supone al Derecho, ocasionó inevitablemente el reconocimiento jurisprudencial del derecho al olvido, para dar satisfacción a situaciones cuotidianas en las que se veían vulnerados derechos tan fundamentales como la intimidad o el honor de los ciudadanos.

Así las cosas, el Tribunal de Justicia concluyó, en su sentencia de 13 de mayo de 2014 (*Google Inc. versus Agencia Española de Protección de Datos*), más conocida como "caso Google", la existencia de un derecho al borrado de nuestra información en Internet. Es aquí cuando se gesta el derecho al olvido bajo la premisa de que las restricciones tecnológicas no pueden servir de excusa para las intromisiones ilegítimas

[17] Sin embargo, se encuentran referencias de hace más de tres décadas en manos de SALVADOR CODERCH quien, a propósito de la famosa sentencia *SIDIS v. F.R. Publishing Corp*, reflexionaba acerca de la intromisión en la privacidad de los personajes públicos. SALVADOR CODERCH, PABLO. ¿Qué es difamar? Libelo contra la Ley del Libelo, Civitas, 1987.

en los derechos fundamentales de los ciudadanos en Internet, que deben protegerse en todo caso.

Este derecho al olvido digital se ha construido jurisprudencialmente a partir de derechos tan básicos como la privacidad, la personalidad y el tratamiento de datos personales que, en el ámbito digital, se ven directamente afectados por la memoria electrónica eterna y las acciones de recuperación y compilación que llevan a cabo los buscadores de Internet.

Esta resolución judicial puso de relevancia dos cuestiones que venían defendiéndose por parte de la doctrina, en primer lugar, que un tratamiento de datos personales inadecuado no sólo se produce cuando éstos son inexactos sino que puede tener lugar incluso cuando los datos sean "inadecuados, no pertinentes o excesivos" en relación con los fines del tratamiento, o cuando no estén actualizados o se conserven por un tiempo superior al necesario.
En segundo lugar, puso de relevancia la extensión de la responsabilidad en el tratamiento de datos hacia los gestores de los buscadores en Internet incluso cuando no estén domiciliados en España pero realicen su actividad por medio de un establecimiento permanente sito en ella -como lo es una filial que se dedica a llevar a cabo actividades comerciales y publicitarias para con la primera- por lo que, se permite a los particulares dirigirse directamente ante los buscadores en Internet para ejercer los derechos de rectificación y oposición de sus datos.

Este pronunciamiento jurisprudencial ha supuesto un punto de inflexión en el campo de estudio que venimos presentando y es fruto de la evolución simultánea entre Derecho y sociedad, dónde hoy en día parece prácticamente imposible lograr una desconexión tecnológica por parte del ciudadano, que muchas veces no puede prescindir de Internet[18] y necesita ver igualmente sus derechos garantizados.

La dependencia de las nuevas tecnologías en nuestra vida diaria es tal que ya han surgido empresas dedicadas única y exclusivamente a hacer desaparecer del

[18] La desconexión tecnológica es hoy día prácticamente imposible: las entidades bancarias remiten a sus clientes a las plataformas online para hacer todo tipo de gestiones, la sanidad pública utiliza la plataforma digital para dar cita a sus pacientes en muchos casos, incluso Hacienda cuenta con una plataforma digital como único medio posible para contestar los requerimientos hechos a los ciudadanos.

ciberespacio a sus clientes, sin embargo, el derecho al olvido es un derecho de todo ciudadano por lo que, con el Nuevo Reglamento Europeo de Protección de datos, y su expresa formulación del "derecho de supresión", se pretende hacer más accesibles y sencillos los procedimientos de borrado de la huella digital en los casos en los que resulte directamente contrapuesto con derechos fundamentales como la intimidad o el honor.

IV. El nuevo Reglamento Europeo de Datos Personales

Siguiendo la lógica sucesiva de los acontecimientos, y con la pretensión de dotar de una mayor seguridad jurídica a los ciudadanos frente a este nuevo panorama, se publicó el 4 de mayo de 2016, 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.

Este Reglamento (de entrada en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea pero sólo aplicable a partir del 25 de mayo de 2018) pretende unificar y modernizar la normativa europea sobre protección de datos, permitiendo a los ciudadanos un mejor control de su información personal.

Las divergencias en la protección de los datos personales entre los Estados miembros en la actualidad son notables a consecuencia, de una parte, de la discordante transposición que los Estados hicieron de la Directiva 95/46/CE que ahora se deroga y, de otra, de la gran cantidad de cláusulas abiertas que contenía (*open-ended-principles*).

Ello, en la práctica, conlleva problemas de regulación en casos tan sensibles como, por ejemplo, en la operatividad de las empresas multinacionales que prestan servicios de redes sociales y que, con la intención de burlar la aplicación de la legislación europea, están radicadas en países más tolerantes con el tratamiento de datos personales y su venta a terceros con fines comerciales (como EEUU). Así, la nueva normativa europea pretende, por una parte reducir el margen de actuación de los Estados miembros en la materia con una intención claramente armonizadora, por otra parte, defender los derechos fundamentales de los ciudadanos con independencia de que las empresas prestadoras de servicios se encuentren domiciliadas o no en territorio europeo.

El Nuevo Reglamento de Protección de datos asume como regla básica el hecho de que nuestra información personal debería estar sometida a nuestro propio criterio, sobre el que tener cierto grado de control, lo que consecuentemente obliga a las empresas operadoras de Internet a encaminar sus actuaciones hacia la protección de los derechos de los usuarios (por ejemplo, se les impone el deber de realizar evaluaciones de impacto, establecer códigos de conducta, nombrar un delegado de protección de datos…) haciéndoles incluso responsables activos en la gestión de la información personal.

Con la intención de dotar al ciudadano de un mayor poder sobre su información personal, se reconoce el derecho a la portabilidad de los datos de forma que todo usuario podrá solicitar que se retiren de Internet los datos personales que ya no sean necesarios para la finalidad con la que fueron inicialmente recogidos, incluso si se tratase de informaciones obsoletas o irrelevantes.

Sin embargo, la medida más destacable del Reglamento es que extiende su aplicación territorial a los responsables no establecidos en la UE cuando las actividades de tratamiento de datos personales estén relacionadas con la oferta de bienes o servicios a interesados que residan en la UE o que ejerzan su actividad en ella, acabando de una vez por todas con la disparidad de criterios entre los distintos órganos jurisdiccionales en cuanto a aspectos tan importantes como la legitimación pasiva de los intervinientes.

Se trata de poner fin así al problema de la falta de territorialidad que tanto dificulta la actuación de los poderes legislativo y judicial, acabando por fin con el argumento esgrimido por la mayoría de corporaciones internacionales que acostumbran a alegar la falta de aplicabilidad del Derecho europeo para eludir sus obligaciones, obligando además a los ciudadanos a pleitear en tribunales estadounidenses, dado que han establecido sus sedes en países con una legislación más favorable a la mercantilización de los datos de sus usuarios, lo que, en la práctica, ha supuesto la universalización de la jurisdicción estadounidense a los asuntos de Internet[19], incumpliendo sistemáticamente

[19] La legislación europea es más proteccionista respecto de la divulgación de la información personal por lo que nuestros datos personales están casi enteramente en compañías establecidas en Estados Unidos dónde se ha producido un éxodo masivo de las corporaciones que operan en Internet.

las legislaciones locales como la española en las que no tienen su sede principal, y acabando con los "estados-nación".

Otra medida estrella de la nueva normativa es, como ya se ha adelantado antes, el reconocimiento, por primera vez y de forma expresa en el artículo 17, del derecho al olvido tal y como había reparado el TEDH, al que renombra como "derecho de supresión". Y lo hace configurándolo como una suerte de derivación del derecho a la intimidad y a la propia imagen y como extensión del derecho al honor.
Se codifica así un derecho que hasta ahora había sido una creación jurisprudencial, permitiendo al interesado obtener "sin dilación indebida" el borrado de sus datos personales de Internet por causas justificadas o porque con el paso del tiempo han perdido su virtualidad.

La voluntad del Reglamento reside claramente en amparar a los ciudadanos en sus derechos, para ello incluso se ha creado un procedimiento de ventanilla única que pretende eliminar toda traba burocrática que impida el debido cumplimiento de sus disposiciones, y que permitirá a los ciudadanos dirigirse a la Autoridad nacional competente (la AEPD, en nuestro caso) para solicitar el amparo de sus derechos.

Finalmente, señalar que el Reglamento regula un aumento de las sanciones de forma muy notable e introduce el concepto de "*accountability*" que implica que no sólo existe responsabilidad por una infracción, sino que la no adopción de todas las medidas requeridas para el perfecto cumplimiento normativo o la falta de diligencia al hacerlo, supone también una responsabilidad punible para la empresa y/o profesional. Precisamente, el Reglamento, prevé la creación de la figura del Delegado de Protección de datos personales, cuyo cometido es velar por el cumplimiento de la legislación en este sentido, veremos si resulta o no efectivo.

i. ¿Estamos por fin ante un cambio de paradigma?

No cabe duda de que la nueva normativa es mucho más garantista en materia de tratamiento de datos que, por ejemplo, nuestra LOPJ. Si bien esta última no considera necesario el consentimiento del interesado para el tratamiento de sus datos cuando los

mismos se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias, otra novedad del Reglamento es la exigencia del consentimiento expreso del interesado como principio general, en cada uno de los supuestos imaginables. Asimismo, se establece que los datos recogidos para finalidades determinadas, explícitas y legítimas no pueden ser tratados posteriormente de manera incompatible con esos fines, así como la adecuación del tiempo de su conservación que, sólo podrán exceder el periodo previsto para dicha finalidad por motivos de investigación histórica, estadística o científica.

Esto, aunque tiene una lógica indiscutible, parece difícil de conseguir en la práctica y no acaba de verse como las legislaciones nacionales podrán articular mecanismos encaminados a una protección de los derechos de los ciudadanos que se recogen en la nueva regulación, sin caer en atascos burocráticos, ni tampoco cómo va a conseguirse una verdadera homogenización de medidas.

En concreto, nos plantea también algunos interrogantes a los que deberá darse solución en un futuro inmediato como, por ejemplo, cómo se articulará el Reglamento en España en relación con la LOPJ -a la que parece desplazar junto con su reglamento de desarrollo de 2007-, qué ocurrirá a partir de ahora con el registro de ficheros o qué papel jugará a partir de su entrada en vigor la AEPD así como el valor de sus circulares. También cabe plantearse si esto supone el fin de los conocidos como derechos ARCO en España (acceso, rectificación, cancelación y oposición) ya que la nueva normativa se refiere a los derechos de Transparencia, Información, Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de datos y Oposición.

Del mismo modo, nos declaramos escépticos sobre cómo van a reaccionar las corporaciones que hasta ahora operan en el ámbito de Internet y de si las sanciones económicas serán suficientemente disuasorias para cambiar las prácticas comerciales, pues las normas sobre protección de datos parecen a priori incompatibles con la forma de proceder en el Internet de las cosas y de los datos masivos.

También debe tenerse en cuenta que la tecnología en sí misma constituye una limitación para el cumplimiento total de los derechos que allí se comprenden pues, por ejemplo, hasta la fecha no hay manera posible desde un punto de vista técnico, de borrar por

completo y para siempre la información subida a Internet. Es decir, cabe plantearse si esto es técnicamente reversible, si no hemos llegado a un punto de no retorno dada la magnitud de la difusión de nuestros datos personales.

Por último, es ingenuo pensar que la finalidad única del Reglamento sea acabar con la desprotección de los ciudadanos europeos, nada más lejos de la realidad pues lo que realmente pretende evitar es que se continúen produciendo obstáculos para el mercado interior de la UE, lo que dificulta el ejercicio de actividades económicas a escala comunitaria y está provocando un falseamiento de la competencia.

Lo cierto es que no contamos con un instrumento jurídico internacional único, de carácter vinculante, que permita actuar en cualquier lugar del mundo cuando un derecho fundamental como la intimidad, se vea menoscabado. Y de esta falta de jurisdicción (y de territorialidad también pues Internet, por definición, carece de espacio físico) no se benefician los ciudadanos individuales sino que es aprovechado por las empresas que controlan el mercado de Internet para hacer negocio y obtener rendimientos económicos de nuestros datos personales.

ii. Propuestas alternativas de futuro

La tecnología es una invención humana y, en consecuencia, ésta no es imparcial, no funciona de manera autónoma sino que son las personas que le dan uso las que dictan sus posiciones. Así, empresas como WhatsApp o Facebook han tomado la decisión consciente de almacenar cantidades ingentes de datos personales de sus usuarios igual que han resuelto vender esta información a terceros, en beneficio propio y en el marco de una decisión empresarial.

La nueva regulación europea pretende poner fin a ciertas actitudes empresariales que comprometen seriamente los derechos de los usuarios de Internet en particular y de los ciudadanos en general, aunque como se ha visto, quedan muchos flecos por determinar y el nuevo marco normativo parece insuficiente pues necesita de otras herramientas multidisciplinares por lo que podría no ser la solución definitiva.

Ante este panorama, hay quien defiende la autorregulación como instrumento alternativo de control aunque, a tenor de los acontecimientos, no parece ésta una buena idea, al menos no para los ciudadanos y la salvaguarda de sus derechos.
Los partidarios de emplear el *soft law* para regular Internet esgrimen que dada la confianza social en la que se basan los términos de uso, por ejemplo de las redes sociales, el grado de cumplimiento de los mismos es elevadísimo. Sin embargo, esto no es del todo cierto, los usuarios y los prestadores del servicio no están en igualdad de condiciones así como los titulares de los datos personales que allí se manejan no son sus propietarios, las reglas de juego en Internet no son las mismas que en el mundo real aunque las consecuencias que comportan las vulneraciones de derechos transciendan a la realidad offline.

Hasta ahora se ha venido imponiendo en el ámbito de Internet el modelo de la publicidad personal por defecto, fruto de una decisión discrecional de las empresas que operan en el medio que han orientado el mismo hacia la rentabilidad económica en detrimento de los intereses y derechos de los usuarios. Sin embargo nada es eterno y no hay motivo para no cambiar el proceder actual por ejemplo, invirtiendo por completo el planteamiento hasta ahora mantenido.

Es decir, se propone la llamada "privacidad por diseño" como una estrategia más idónea a seguir –y como complemento de la acción normativa y armonizadora planteada por el nuevo marco europeo- a la hora de proteger la intimidad de los ciudadanos que, debido a la configuración por defecto de las páginas web y de sus dispositivos inteligentes resultan cómplices, muchas veces sin saberlo, de prácticas de negocio que menoscaban su privacidad.
Los consumidores deben ser capaces de comprender la utilización que de sus datos personales va a hacerse así como de dar un consentimiento válido para el tratamiento de éstos y en ningún caso los costes de ejercer sus derechos fundamentales pueden exceder a los beneficios de hacerlo.

Una forma de proteger a los usuarios de Internet, pasa por aplicar lo que se ha venido llamando *Privacy by design*, obligando a las empresas operadoras de Internet a ofrecer servicios fáciles de usar y respetuosos con la privacidad. Esto implicaría, por ejemplo, que por el hecho de navegar por ciertas redes o por utilizar determinados servicios de

Internet, no se presuponga que los sujetos autorizan la monitorización de su actividad en la red ni otorgan su consentimiento implícito para el almacenamiento y tratamiento de sus datos personales.

Es decir, se trataría de obligar a las empresas a operar de modo que se dote a los usuarios de una mayor seguridad jurídica, dónde no haya lugar para cláusulas contractuales opacas ni engañosas y garantizando en todo caso la prestación de su consentimiento, sin que dichas corporaciones puedan quedar eximidas de los principios jurídicos más fundamentales excusándose en el empleo de nuevas tecnologías. La tecnología debería de ser neutra, no puede dificultar el ejercicio de derechos que los sujetos tienen reconocidos y vienen ejerciendo en el mundo offline.

Y es que a la persona que se ve expuesta en sus datos privados no se le puede transferir la responsabilidad de hacer desaparecer dicha información, haciéndole que se dirija a una suerte de operadores y empresas de Internet, sino más bien al contrario, deben establecerse mecanismos que permitan, por configuración inicial, que sólo sean objeto de tratamiento los datos necesarios para cada fin específico. Así, por ejemplo, el derecho al olvido no tendría que actuar sólo a instancia de parte, sino que se instauraría como una regla general cuyo funcionamiento fuese automático, por defecto y no sólo bajo petición.

V. Conclusiones

El estado actual de la tecnología es encomiable así como las numerosas ventajas que tiene aparejadas, sin embargo también ha supuesto ciertos riesgos para algunos derechos fundamentales y es que el comercio de los datos personales se ha revelado como un negocio en auge gracias a las modernas tecnologías inteligentes. Las grandes corporaciones obtienen nuestra información personal, principalmente a través de contratos de adhesión de servicios falsamente gratuitos para el usuario y de cláusulas abusivas que constantemente se modifican unilateralmente para dejar menos espacio a la privacidad.

Hay que ser consciente de que durante los últimos años venimos asistiendo a una redefinición de la privacidad, especialmente por el modo en que los particulares exponen su intimidad de forma voluntaria y, con ello, el modo de entender la protección de datos ha variado sustancialmente. No obstante, ello no puede significar una desprotección absoluta de los ciudadanos frente al manejo del Big data, el mercadeo de datos personales debe encontrar sus límites en algún punto.

Bajo el pretexto de la innovación tecnológica no se pueden amparar prácticas abusivas para con ciertos derechos fundamentales que no son ni negociables ni renunciables. La protección de la privacidad requiere de la intervención de la política pública, no es un sector que pueda dejarse a la autorregulación pues hasta ahora, dicho mecanismo se ha revelado enteramente ineficaz, principalmente porque las corporaciones que controlan Internet operan exclusivamente con finalidad de negocio.

Mientras los avances tecnológicos se suceden a una velocidad vertiginosa, los tiempos del legislador son otros y, junto con la prosopopeya política del momento, no se ha sabido dotar a los ciudadanos de protección efectiva ante nuevas vulneraciones para sus derechos. En este contexto, han sido los tribunales, tanto nacionales como supraestatales, los que han jugado un papel esencial en el amparo de las garantías ciudadanas no exentos, sin embargo, de dificultades procesales en el camino.

Este panorama puede cambiar con la nueva regulación europea en la materia y, aunque habrá que esperar a su aplicación definitiva -en mayo de 2018- y a la armonización de las legislaciones nacionales en este sentido, el nuevo Reglamento Europeo de Protección de Datos se ha fijado como objetivo acabar con las prácticas empresariales indiscriminadas que hasta ahora vienen ignorando las legislaciones domésticas en materia de privacidad y protección de datos. El texto, mediante criterios unificadores y extensivos, trata de poner fin al problema de la falta de territorialidad, jurisdicción y ley aplicable que dificultan la garantía de tales derechos, aplicándose a partir de ahora no sólo a los responsables o encargados del tratamiento de datos establecidos en la UE sino también a aquéllos otros que, sin estar domiciliados en ella, lleven a cabo tratamiento de datos respecto de ciudadanos europeos. También, con el objetivo de acabar con la memoria digital eterna, se regula expresamente el “derecho de supresión” (comúnmente

denominado derecho al olvido) para los casos en los que resulte directamente contrapuesto con derechos fundamentales como la intimidad o el honor.

No obstante, este texto no está exento de críticas, tanto respecto de su futura efectividad como debido a las motivaciones que han dado lugar a su alumbramiento. Tampoco parece capaz de poner freno al problema de fondo que tiene su origen en el cambio, en términos sociales y tecnológicos, del modo de entender la privacidad.

Habría que ir un paso más allá y adelantarse a futuros acontecimientos, redefiniendo los límites, el significado y el alcance de los derechos clásicos de intimidad y protección de datos para encontrar así un equilibrio que permita el desarrollo tecnológico y la supervivencia de los derechos fundamentales de las personas, dotando de seguridad jurídica a todas las partes implicadas. Por el contrario, siempre nos quedará la opción de renunciar a las comodidades que nos ofrecen las innovaciones tecnológicas a cambio de preservar nuestra privacidad aunque, siendo sinceros, eso no parece muy realista.