GARANTÍAS LEGALES DEL CONCEPTO DE PRIVACIDAD: ENTRE EL DERECHO AL OLVIDO Y EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

LEGAL GUARANTEES OF THE CONCEPT OF PRIVACY: BETWEEN THE RIGHT TO BE FORGOTTEN AND THE NEW GENERAL DATA PROTECTION REGULATION

Actualidad Jurídica Iberoamericana Nº 9, agosto 2018, ISSN: 2386-4567, pp. 176-201

Marina
SANCHO
LÓPEZ

ARTÍCULO RECIBIDO: 3 de mayo de 2018
ARTÍCULO APROBADO: 30 de junio de 2018

RESUMEN: El funcionamiento de las nuevas tecnologías y el suministro de bienes digitales, comporta para los usuarios revelar sus datos personales, la compraventa de los cuales es ya una realidad, con el peligro que ello supone para la privacidad de los ciudadanos. El nuevo Reglamento Europeo de Protección de Datos ha creado un nuevo marco jurídico que pretende dar un giro radical al modelo actual, dotando a los usuarios de mayores potestades para el control de sus datos. Muestra de ello es la formulación, expresa y por primera vez, del derecho al olvido, que permite a los ciudadanos el borrado digital de sus datos cuando se pongan en peligro otros derechos fundamentales.

PALABRAS CLAVE: Derecho y nuevas tecnologías; privacidad; Big data; derecho al olvido; Internet.

ABSTRACT: *The operation of new technologies and the supply of digital goods involves for users to disclose their personal data. The market data is already a reality with the danger that this entails for the privacy of citizens. The new General Data Protection Regulation has created a new legal framework that aims to radically change the current model, giving users greater powers to control their data. A good example of this is the express statement, and for the first time, of the right to be forgotten, which allows citizens to digitally erase their data when other fundamental rights are endangered.*

KEY WORDS: *Law & new technologies; privacy; Big data; right to be forgotten; internet.*

I. INTRODUCCIÓN.

Aunque el término Sociedad de la Información ha caído en desuso, no hay mejor definición para entender el actual fenómeno de nuestro entorno socio digital en relación a las nuevas tecnologías de Internet, que han revolucionado nuestra forma de comunicarnos en sociedad, así como ciertos patrones económicos, culturales, de consumo y hasta nuestras pautas de comportamiento.

En nuestro día a día compartimos constantemente cantidades ingentes de información, y del mismo modo, podemos acceder inmediatamente a grandes bases de datos en cualquier momento y prácticamente desde cualquier dispositivo electrónico conectado a Internet. Una vez los datos son incorporados a la Red, circulan libremente por el ciberespacio pasando de unas bases de datos a otras y de un servidor de Internet a otro por lo que, si además tenemos en cuenta las copias periódicas que se hacen de las páginas web, incluso consiguiendo borrar la información de su fuente original, resultaría prácticamente imposible hacerla desaparecer de todos los rincones del ciberespacio. Esto ha sido bautizado por el Prof. Troncoso como el "efecto Hotel California": *you may enter, but you may never leave*[1].

Entre todos esos datos que circulan por la Red, existe una cantidad ingente de datos de carácter personal, cuya naturaleza los hace especialmente sensibles, precisamente por su capacidad de identificarnos. Así, este tipo de datos, por el volumen de información que son capaces de aportar, se han revelado como un negocio en auge, revolucionando la mercadotecnia y las estrategias del marketing

1 Troncoso Reigada, A.: *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, València, 2008, p. 320.

• Marina Sancho López
Investigadora Contratada de Derecho Civil de la Universidad de Valencia, marina.sancho@uv.es

personalizado eso sí, con consecuencias negativas para algunos derechos fundamentales.

Resulta curioso que el valor de los bienes, tradicionalmente basado en su escasez y en su demanda, haya cambiado radicalmente su lógica en Internet y pase a considerarse ahora valioso por el gran volumen de información que circula por ella, algo expresado hace años por la Ley de Metcalfe[2] cuando se trataba de explicar el valor potencial de la tecnología de Ethernet.

Recientemente, Tim Berners-Lee, inventor de la World Wide Web, con motivo del 28 aniversario de su hazaña, reflexionaba[3] sobre el papel actual de Internet y reclamaba una mayor ética en su uso, reivindicando el papel de la Web como un servicio que debe beneficiar a toda la humanidad. En su carta abierta se muestra principalmente preocupado por la pérdida de nuestra información personal en Internet y por la utilización de ésta junto con algoritmos matemáticos para, por ejemplo, incentivar el consumo de sus usuarios o para hacer campañas políticas capaces de, persuadir a potenciales votantes mediante su redirección hacia sitios de "fake news" (noticias falsas), ahora de gran actualidad.

II. LOS NUEVOS TIEMPOS PARA LA PRIVACIDAD.

La tecnología e Internet han revolucionado por completo nuestra forma de concebir la vida. Vivimos en un momento de cambio constante, donde la técnica no se detiene y dónde un solo pestañeo puede alejarte de la vanguardia; usando la terminología de Bauman[4], vivimos en una época de "modernidad líquida".

En esta nueva etapa se produce un cambio radical en la cohabitación humana, en el condicionamiento social de las políticas de vida. Conceptos como la velocidad del movimiento o el espacio han dado un giro radical hasta diluir sus fronteras llegando incluso a desaparecer. Así, por ejemplo, los avances tecnológicos han logrado una instantaneidad en la comunicación que ha supuesto la eliminación de la concepción del espacio como límite de las relaciones sociales, pues nuestros actos ya no se circunscriben al entorno más inmediato, sino que van más allá del espacio físico. Se produce aquí una confusión entre el entorno "offline" y el

2 La Ley de Metcalfe, creada por Robert Metcalfe, cuyo enunciado consiste en "El valor de una red de comunicaciones aumenta proporcionalmente al cuadrado del número de usuarios del sistema (n2)", trata de ilustrar cómo el crecimiento exponencial de los usuarios de una red puede aumentar considerablemente su valor, cosa que ejemplifica el valor económico de una tecnología aplicada a las telecomunicaciones.

3 http://webfoundation.org/2017/03/web-turns-28-letter/.

4 Bauman, Z.: *Modernidad líquida*, Fondo de Cultura Económica, México, 2000.

"online" que, como consecuencia de la interconexión actual, hace muy difícil una separación radical entre ambas realidades que a menudo se yuxtaponen[5].

Desde hace un tiempo, venimos asistiendo a un vertiginoso cambio tecnológico-social hasta el punto de que impera la sensación de transición constante que, sin embargo, no se ha traducido significativamente al Derecho, incapaz de adaptarse al nuevo paradigma ni de anticiparse a realidades futuras. Un ejemplo claro sería la noción de "Estado" o "frontera", totalmente superado por la realidad de Internet, de jurisdicción mundial si cabe, cuyo poder territorial carece de sentido hoy día, por ejemplo, ante casos de vulneraciones de derechos en las transferencias internacionales de datos personales.

La modernidad líquida y la mutabilidad que conlleva originan en la sociedad la sensación permanente de volatilidad, lo que ciertamente supone incertidumbre y claro está, inseguridad jurídica. Esta nueva realidad incita a repensar y reconfigurar conceptos que indudablemente han adquirido un nuevo significado, como "intimidad", "vida privada" o de "lo público" y "lo privado".

Ni las nuevas tecnologías ni Internet han creado nuevos bienes jurídicos protegidos, ni sustanciales cambios en los principios y valores del ordenamiento jurídico, pero, sin embargo, sí que han aumentado exponencialmente las vulneraciones de derechos así como creado nuevas formas de lesión. Frente a este nuevo escenario, se exige una reacción proporcionada por parte del Derecho, que dote de mecanismos jurídicos adecuados para sufragar nuevas realidades, reconociendo nuevos derechos capaces de reflejar nuevas necesidades, si fuera necesario.

En la relación entre la tecnología y el Derecho, se parte de presupuestos contrapuestos, si bien este último se caracteriza –desgraciadamente- por su lentitud a la hora de reaccionar ante nuevos fenómenos sociales y jurídicos, una vez lo hace, pronto queda superado por el devenir de los acontecimientos ya que la informática y la tecnología están en continua evolución, condenando los procedimientos de tutela jurídica al anacronismo.

Internet ha supuesto un nuevo paradigma para la privacidad de las personas y sus derechos derivados en tanto que tiene un efecto multiplicador de los atentados que contra éstos puedan tener lugar. La exposición masiva de información, accesible desde cualquier punto del planeta, ha creado un ambiente propicio para

5 Hoy en día, muchas de las acciones que tienen lugar en Internet tienen consecuencias evidentes en el entorno "físico" y viceversa. Un ejemplo de relevante actualidad es la persecución de aquellas conductas de enaltecimiento del terrorismo perpetradas mediante el uso de redes sociales que están derivando en auténticas condenas penales.

perpetrar vulneraciones de derechos fundamentales como la igualdad, la intimidad, la dignidad, la libertad, la propia imagen o el honor.

Esto se debe principalmente a la injerencia del Big data -llamamos Big data al almacenamiento, tratamiento y transferencia de datos a gran escala a través de las tecnologías de Internet- en las nuevas relaciones sociales y comerciales, pues las nuevas tecnologías inteligentes funcionan a partir de datos y metadatos -datos sobre los propios datos- que se consiguen, generalmente, bien a través de las aplicaciones descargadas en los dispositivos o bien directamente proporcionados por los usuarios.

El uso o la instalación de la mayoría de servicios y aplicaciones informáticas aparentemente gratuitas suponen auténticos contratos de adhesión – con un alto número de cláusulas abusivas, por cierto- dónde los usuarios ceden sus datos personales – en ocasiones sin autorización expresa o incluso sin su conocimiento[6]- en contraprestación por los servicios recibidos, que más tarde se monetizan por dichas empresas dedicadas, en el fondo, al almacenaje, tratamiento, exportación y venta de datos personales.

El hecho de que Internet no suponga un coste económico o que ciertas aplicaciones sean "gratis" no es razón suficiente para no exigir un respeto íntegro de los derechos fundamentales en este ámbito[7], cuando además se está partiendo de una premisa incorrecta pues, ni esos servicios son gratuitos (tienen un coste: la privacidad de sus usuarios, la cesión de los datos integran dicha contraprestación) ni muchas veces son voluntarios, pues no existen alternativas a la utilización de dichos servicios (son muchos los trámites que requieren el uso de plataformas online como por ejemplo, la Agencia Tributaria o la Seguridad Social[8]).

Internet no cuenta con un competidor directo pues los medios tradicionales quedan integrados en su funcionamiento, ampliando su difusión exponencialmente. Además, y por definición, Internet tiene un alcance ilimitado y transnacional lo que dificulta enormemente la persecución aquellas conductas vulneradoras

6 Mientras que la legislación tradicional sobre protección de datos está principalmente basada en aquellos datos qué los usuarios comparten o ceden de manera voluntaria, lo cierto es que, en la práctica, éstos son los menos en comparación con el gran volumen de datos y metadatos que se extraen diariamente sin que los usuarios tengan conocimiento y, claro está, dichas acciones no cuentan con su consentimiento.

7 Debe superarse de una vez por todas el argumento de que, como son los particulares quienes deciden voluntariamente ceder parte de su privacidad a cambio de poder utilizar ciertos servicios, éstos renuncian a una serie de derechos que, en otras circunstancias les serían aplicables. Habría que plantearse aquí, hasta qué punto los individuos pueden transigir con la intimidad y la propia imagen, pues recordemos que son derechos de la personalidad inherentes a la dignidad personal y fundamentalmente y por definición, intransmisibles e irrenunciables.

8 También cabría preguntarse hasta qué punto puede prescindirse de ciertos servicios cuyo uso es voluntario, como por ejemplo WhatsApp, pues hoy en día para estar conectado en sociedad es prácticamente una herramienta imprescindible y tal y como concebimos la comunicación en el presente, los usuarios de su servicio de mensajería nos vemos incapaces de prescindir de sus servicios por lo que, aceptamos sus términos de uso incluso sabiendo cuáles son las consecuencias para nuestros datos personales.

de derechos, si tenemos en cuenta además la disparidad de operadores que intervienen en su gestión: los proveedores de red, de acceso o de servicio, los creadores de un contenido que ha dado lugar a dicha vulneración, quienes han permitido su acceso y difusión, o los usuarios que reproduzcan de nuevo su contenido… Muchos de los cuales pueden estar radicados en lugares distintos y sometidos a legislaciones dispares, lo que se conoce como "deslocalización".

Es curioso cómo se tiene la creencia generalizada de que Internet incrementa la libertad de las personas mientras que, ante un supuesto de vulneración de derechos, esas "virtudes" se convierten en impedimentos para lograr la restitución de la situación y, aún más, para exigir responsabilidades ante dicho incumplimiento. Esa es la gran paradoja de Internet, la contraposición entre la facilidad con la que la información fluye por la Red de forma ilimitada -paradigma de la libertad de expresión e información- y la dificultad de eliminar aquél contenido que produce una lesión de derechos fundamentales, por la propia lógica de funcionamiento del sistema.

Y es en este entorno online, ajeno a los límites territoriales que protegen los datos personales dentro de sus jurisdicciones, y gracias a la técnica, donde se ha posibilitado que las empresas que operan online abusen de los datos personales de los usuarios, convirtiendo las normativas nacionales y europeas en papel mojado.

Además de una evidente pérdida de privacidad, otra de las consecuencias inmediatas que tiene lugar con la cesión y el almacenamiento masivo de datos, es la monitorización de los individuos. El control al que estamos sometidos los ciudadanos no tiene precedentes históricos pues, con la informatización de las Administraciones públicas y la digitalización de nuestros datos personales nos encontramos en un escenario, inimaginable veinte años atrás.

Desde la tarjeta sanitaria con la que ahora podemos pedir cita y acudir a la farmacia para que nos den los medicamentos hasta la posibilidad de hacer la renta por Internet, pasando por el registro de las transacciones comerciales que realizamos con las tarjetas de crédito o vía Internet. Todo ello, que indudablemente facilita el día a día y agiliza las transacciones cuotidianas, conlleva un control social del que es muy difícil escapar y que asumimos como inevitable, pese a que desconocemos todas las implicaciones negativas que pueda conllevar.

Lo que se denominó por Frosini[9] "juicio universal permanente" hace más de treinta años, y que algunos tildaron de conspiracionista, hoy en día y teniendo en cuenta todos los aparatos electrónicos que monitorizan nuestra vida cuotidiana, este concepto vuelve a estar de plena actualidad, pues los ciudadanos nos

9 Frosini, V.: *Cibernética, derecho y sociedad*, Tecnos, Madrid, 1982, p. 178.

encontramos sometidos a una vigilancia permanente e inadvertida que, con ayuda de las últimas invenciones, va ampliando su ámbito de permeabilidad en nuestra privacidad, en la práctica, casi inexistente.

Cuanto más extensa es la innovación tecnológica y cuanto mayor sea su generalización, menor es el ámbito de privacidad reservado a los individuos, lo que consecuentemente se traduce en un potencial riesgo para la libertad y la igualdad en lo que Pérez Luño[10] ha denominado "asalto tecnológico de los derechos y libertades", donde resulta difícilmente negable la injerencia de la informática de control individual y colectivo que comprometen gravemente valores como la identidad, dignidad e igualdad.

Los abusos acometidos por la informática y la telemática, a veces indetectables, penetran en el devenir social y cultural hasta el punto de no cuestionarnos esta realidad que asumimos como propia[11], mientras que en la esfera jurídica se empiezan a manifestar las consecuencias negativas de este modelo actual. Un modelo en el que la tecnología, que no es neutral, se ha inclinado por la comercialización de los datos personales, preconfigurando los dispositivos electrónicos inteligentes para monitorizar la actividad de los usuarios: sus contraseñas, sus rutinas de conexión, su localización, sus hábitos de consumo… convirtiendo información tradicionalmente privada en no tan privada y al servicio de la mercadotecnia.

De este modo, cuando hablamos de las corporaciones del Big data nos referimos a las industrias, incluidas la banca, las aseguradoras, las empresas de telecomunicación o de marketing, que emplean datos personales para el funcionamiento de sus servicios, así como para customizar los productos o minimizar el fraude lo que, consecuentemente, comporta un verdadero peligro de discriminación.

Si bien es cierto que la legislación española en materia de datos personales es bastante garantista y exige el consentimiento inequívoco del titular de la información personal -que a su vez deberá de conocer expresamente la finalidad del tratamiento de sus datos- así como la autorización para la cesión de éstos a terceros, en el ámbito de Internet y las empresas que operan en él, es prácticamente imposible saber cuándo estamos siendo monitorizados y qué usos posteriores se le va a dar a nuestra información más personal.

10 Pérez Luño, A. E.: *Los derechos humanos en la sociedad tecnológica*, Universitas, Madrid, 2012, p. 23.

11 Este fenómeno ha sido descrito por Solove como "the norm police" para ilustrar como las normas sociales, entendidas como pautas de comportamiento, son el principal mecanismo en que una sociedad ejerce el control social. Un ejemplo de ello lo encontramos en las redes sociales que permiten a golpe de click, por un lado, decidir quién y cómo se adapta al patrón social, y por otro lado, permiten una exposición pública no deseada así como eventuales escarnios o humillaciones públicas. Solove, D. J.: *The future of reputation*, Yale University Press, New Haven and London, 2007, p. 6.

Esto tiene lugar principalmente porque, como se ha dicho ya, la jurisdicción de Internet es universal y no entiende de fronteras, y las grandes corporaciones del Big data han situado sus empresas en jurisdicciones menos proteccionistas con la privacidad de los usuarios, como la estadounidense. Pero ocurre, además, que la exposición en la red tiene un valor añadido y es la permanencia de la historia. En Internet, parece no existir la desmemoria, pues hechos pasados siguen al alcance de todos para quien los desee consultar y se une permanentemente a una persona con hechos pretéritos por lo que difícilmente podrá escapar de su pasado ni lograr el anonimato.

En definitiva, la regulación de la información personal, afecta a los patrones de intercambio de información: cómo las personas individuales expresan su identidad, como las empresas diferencian mercados, y como los gobiernos manejan el riesgo. La interdependencia internacional, principalmente por la expansión de la comunicación, el comercio más allá de las fronteras, y los mercados financieros globales, han transformado las antiguas barreras domésticas en un debate de escala internacional[12] donde las políticas de privacidad tienen grandes implicaciones en la libertad individual, los poderes del estado y la economía global.

Si añadimos a estos factores al desarrollo de las nuevas tecnologías, el funcionamiento de Internet y la enorme autorregulación del sector, es indiscutible la necesidad de medidas políticas, jurídicas y empresariales capaces de lograr un entorno satisfactorio para los derechos en juego, atendiendo a que el flujo de información personal deviene imprescindible.

Asumiendo pues, por un lado, la nueva realidad digital y la expropiación de la privacidad que ha supuesto para los ciudadanos la connivencia del Big data y las nuevas tecnologías, el Reglamento Europeo de Protección de Datos introduce un nuevo marco jurídico con la intención de configurar la protección de los datos personales desde un nuevo punto de vista, dotando a las personas físicas de un mayor control sobre su información personal. Así, la nueva normativa europea ha previsto la creación del derecho de supresión, comúnmente conocido como derecho al olvido, que permite obtener a todo interesado el borrado digital de sus datos personales cuando concurran ciertas circunstancias, cristalizando al fin un derecho de creación jurisprudencial, así como las exigencias doctrinales.

III. EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS.

Teniendo en cuenta las circunstancias anteriores mencionadas y con la pretensión de dotar de una mayor seguridad jurídica a los ciudadanos frente

12 Newman, A. L.: *Data privacy and the global economy*, Cornell University Press, New York, 2008, p. 40.

a este nuevo escenario, 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 (RGDP en adelante), de aplicación efectiva a partir del 25 de mayo de este mismo año.

1. Principales novedades.

Por primera vez en la historia, todos los países de la Unión Europea quedan sometidos a una misma regulación en materia de protección de datos personales, sin que sea necesaria su intervención legislativa para la aplicabilidad de los derechos que conlleva.

La nueva normativa asume como regla básica el hecho de que nuestra información personal debe estar sometida a nuestro propio criterio, la publicación de esta normativa ha supuesto un cambio radical en materia de protección de datos que ahora dota al titular de los datos de todo tipo de derechos para facilitar la gestión de su información personal en base a sus preferencias, y somete a empresas privadas y administraciones públicas al interés del ciudadano, obligándoles a adoptar políticas activas de protección de datos y cambiando las reglas de juego existentes.

La nueva normativa moderniza y unifica el derecho a la protección de los datos teniendo en cuenta el nuevo escenario tecnológico y tratando de acabar con las existentes discrepancias entre los Estados miembros a consecuencia, principalmente de la gran cantidad de cláusulas abiertas que contenía (*open-ended-principles*), que dieron como resultado una trasposición divergente en las distintas normas europeas. Con una voluntad claramente integradora, se trata así de poner solución a los problemas existentes de regulación que en nada favorecía a la protección de los derechos fundamentales, dotando a las empresas operadoras de Internet de nuevas obligaciones, así como reduciendo el margen de actuación de los Estados miembros.

Otra de las grandes novedades del RGDP es que trata de poner fin al problema de falta de territorialidad a través de la extensión de la aplicabilidad de su articulado hacia aquellos responsables que no estén establecidos en la UE cuando las actividades de tratamiento de datos personales estén relacionados con la oferta de bienes o servicios a interesados que residan en suelo europeo o que ejerzan su actividad en éste (artículo 3), acabando de una vez por todas con la disparidad de criterios entre los distintos órganos jurisdiccionales respecto de cuestiones tan importantes como la legitimidad pasiva de los intervinientes.

Con la extensión de su aplicación territorial se pretende subsanar las trabas existentes a la actuación de los poderes legislativo y judicial, y poner fin a la práctica consolidada entre las corporaciones de Internet de establecer sus sedes en países cuyas legislaciones permiten sin demasiados problemas la mercantilización de la información personal, ignorando reiteradamente la legislación doméstica y europea en la materia e impidiendo el ejercicio eficaz de los derechos de los ciudadanos a quienes dejaba en una situación jurídica de indefensión.

Así pues, el artículo 29 obliga a estas empresas a someterse al Derecho de la Unión y a los tribunales nacionales de los Estados miembros cuando ofrezcan sus servicios en suelo europeo, constriñendo la actuación de las mismas en el intento de cumplir con sus obligaciones.

Esta nueva normativa pretende hacer realidad el "habeas data" de los ciudadanos, permitiéndoles un mejor control de su información personal, así como dotándolos de instrumentos efectivos para el cumplimiento de sus derechos.

Un ejemplo claro lo encontramos en la extensión de las obligaciones de su articulado tanto a los responsables como a los encargados del tratamiento de datos, estén o no radicados en la Unión (artículo 3). Mediante la introducción del concepto de "responsabilidad activa", se obliga a unos y a otros a que adopten todas las medidas necesarias para cumplir con los principios, derechos y garantías que se recogen en el RGPD, responsabilizando a ambos de la gestión de la información personal (artículo 24), todo ello junto a numerosas obligaciones encaminadas hacia la protección de los derechos de los usuarios, entre otras, estableciendo códigos de buenas prácticas, realizando evaluaciones de impacto, introduciendo políticas de protección de datos por defecto o nombrando un Delegado de Protección de Datos.

Se recogen, asimismo, los tradicionales derechos ARCO (acceso, rectificación, cancelación y oposición) con significantes modificaciones. Así, por ejemplo, se simplifican las fórmulas para facilitar al interesado el ejercicio de sus derechos de rectificación (artículo 13), se dispone el derecho de todo interesado a obtener una copia de los datos personales objeto del tratamiento (artículo 15), se introduce el derecho de bloqueo de datos como como variante o alternativa al derecho de cancelación (artículo 19), se prevé la posibilidad de limitar el tratamiento de los datos (artículo 18) y se refuerza el derecho de oposición introduciendo nuevos motivos como la elaboración de perfiles (artículo 21).

Para dotar de mayor virtualidad al control de los ciudadanos de su propia información personal se reconoce expresamente el derecho a la portabilidad de datos (artículo 20), permitiendo a todo usuario solicitar en cualquier momento la retirada de Internet de aquéllos datos personales que ya no sean necesarios para

las finalidades iniciales por las que fueron recogidos, del mismo modo que si se trata de informaciones obsoletas o irrelevantes.

Entre los derechos de nueva incorporación destaca preeminentemente el derecho de supresión, popularmente conocido como el derecho al olvido (artículo 17), permitiendo a todo interesado obtener "sin dilación indebida" el borrado de sus datos personales cuando concurran ciertas circunstancias, codificando así un derecho hasta entonces de creación jurisprudencial.

Para facilitar el ejercicio de estas potestades se dispone que los responsables posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se lleve a cabo por estos canales (artículo 15). De igual forma, el ejercicio de dichos derechos será preeminentemente gratuito (artículo 12).

Asimismo, el RGPD incorpora nuevas herramientas de control como el cifrado o la anonimización de los datos personales (artículo 32), evitando de forma irreversible la identificación de los sujetos; la seudonimización, consistente en reemplazar un atributo en un registro por otro de manera que la persona sólo puede ser identificada mediante otro mecanismo indirecto (artículo 25); la obligación de realizar una evaluación de impacto (*Privacy Impact Assessment*) cuando se lleve a cabo un tratamiento de datos que pueda conllevar un alto riesgo para los derechos y libertades de las personas físicas (artículo 35) o mediante la aplicación de otras medidas de seguridad (artículo 32)[13].

Por último, se contemplan actuaciones preventivas encaminadas a cumplir con las disposiciones de su articulado, como se extrae de la inclusión de la protección de datos desde el diseño y por defecto como orientación de las políticas y decisiones empresariales que deben llevar a cabo los encargados de cualquier tratamiento de datos personales (artículo 25) como regla general y desde el origen. Junto a este extremo, se introduce el concepto de responsabilidad proactiva (*accountability*) que exige a los encargados la adopción de medidas suficientes para garantizar un tratamiento lícito (artículo 5.2) y exige transparencia en los procedimientos para salvaguardar el ejercicio de los derechos del interesado (artículo 12).

2. Consideraciones críticas.

En cuanto a los aspectos formales, la normativa plantea algunas preguntas acerca de su engranaje con las legislaciones domésticas en materia de protección de datos, en nuestro caso concreto, cómo se articularán los derechos de

13 El RGPD ya no distingue entre ficheros de nivel básico, medio o alto, sino que impone medidas de seguridad en base al estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y las libertades concretas de las personas físicas.

Transparencia, Información, Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad de datos y Oposición del Reglamento con los tradicionales derechos ARCO (Acceso, rectificación, cancelación y oposición) de la doctrina española, qué ocurrirá a partir de ahora con el registro de ficheros, qué papel jugará la Agencia Española de Protección de Datos (AEPD) así como el valor de sus circulares, y cómo se articulará el Reglamento con la LOPJ, mucho menos garantista en comparación con la nueva normativa.

De momento, sólo podemos contestar a esta última pregunta y no del todo, pues si bien el legislador español decidió dictar una nueva normativa española de protección de datos, a la vista de las incompatibilidades de la LOPJ con el Reglamento, ya parece inevitable que la nueva legislación no llegue a tiempo para el 25 de mayo –recordemos, fecha de entrada en vigor del RGPD-, pues el Anteproyecto de Ley todavía está en fase de tramitación parlamentaria. Para lo demás habrá que esperar.

En cuanto a los aspectos sustantivos, resulta llamativo como, pese a establecer ciertos principios programáticos en la norma que sugieren un cambio de modelo –proponiendo políticas de privacidad desde el diseño o facilitando el control por parte del ciudadano de sus propios datos- la normativa adolece de cierto continuismo, introduciendo medidas fragmentarias y dejando nuevamente mucho margen para la interpretación, debido al abuso de conceptos ambiguos y jurídicamente indeterminados.

Esta complejidad terminológica lleva aparejada la introducción de la figura del Delegado de Protección de Datos, presentada como medida estrella de seguridad, pero que en la práctica supondrá cierta arbitrariedad en las decisiones que éstos tomen, y que dependerá de los términos en que se lleve a cabo la interpretación de unos o de otros. Sin embargo, parece una obviedad que el alcance de un derecho fundamental deba delimitarse en términos objetivos y de un modo global y no en base a la opinión de ciertos expertos, dejando un peligroso margen para la autonomía privada.

En relación a lo anterior, el nuevo Reglamento asume como regla básica que la información personal debe estar sometida al control del interesado, a quien dota de un mayor dominio para que gestione sus datos conforme a su propio criterio. Sin embargo, estas medidas de autogobierno presuponen la existencia de una concienciación y responsabilidad ciudadana que, desgraciadamente, dista mucho de la realidad -sólo hay que ver cuántos usuarios leen las políticas de privacidad de las aplicaciones o servicios que usan a diario-, y a quién no se le puede exigir conocimientos jurídico-técnicos para ello.

Entendemos que, para que se trate de una medida ciertamente proteccionista, de ningún modo puede transferírsele a aquella persona que se vea expuesta en sus datos personales la responsabilidad de gestionar dicha situación, haciéndole dirigirse a una suerte de operadores y empresas de Internet. Todo lo contrario, deberían establecerse mecanismos que efectivamente impongan medidas respetuosas con la privacidad desde el origen, cuyo tratamiento de datos se minimice y se constriña a fines específicos, y no recaiga en la responsabilidad individual ni del interesado ni del Delegado de Protección de Datos.

Así, por ejemplo, el derecho al olvido se debería de establecer automáticamente y como regla general cumplidos unos requisitos previos, y no limitar su operatividad bajo petición, dejando en manos y a instancia del interesado su ejecución.

Todo ello, junto con el relego del establecimiento de la mayoría de los procedimientos para el cumplimiento del articulado en manos de los legisladores domésticos, difiere notablemente de la voluntad homogeneizadora del legislador europeo.

En cuanto a su operatividad, el cumplimiento del Reglamento exige unos medios, así como una preparación, dedicación y control constante por parte de las organizaciones que traten con datos personales, cuya aplicación efectiva parece en ocasiones imposible, pues incrementa exponencialmente sus esfuerzos burocráticos, lo que resultará especialmente gravoso para las PIMES y los autónomos.

Así, por ejemplo, el tenor literal de alguna de sus disposiciones exige contar con el consentimiento expreso del interesado para cada uno de los supuestos imaginables de tratamiento de sus datos personales.

Parece dudoso que este esfuerzo burocrático se traduzca efectivamente en un cambio sustancial para la privacidad de los ciudadanos pues, junto a las muchas cuestiones abiertas que no encuentran solución en la nueva normativa, ésta no parece contar con la connivencia de las grandes corporaciones del Big data. Así, por ejemplo, se plantean interrogantes acerca de cómo se aplicará el GDPR en "la nube", muchas veces lejos del control de las empresas y objeto de duplicados. En teoría, a partir de ahora, deberá de tenerse pleno dominio sobre los datos vertidos en dicha plataforma para, por ejemplo, poder ejecutar derechos como el de supresión, con independencia de que se subcontrate a un tercero la responsabilidad del cumplimiento del GDPR.

En otro orden de cosas, resultaría ingenuo pensar que la finalidad última de esta nueva normativa es proteger a los ciudadanos y a sus datos personales frente a las amenazas del Big data pues resulta bastante obvio que el propósito del

GDPR es sentar las bases para lograr un mercado digital único y evitar que se continúen produciendo obstáculos para el mercado interior de la Unión Europea -que, en la práctica, está dificultando el ejercicio de actividades económicas a escala comunitaria- y acabar con el falseamiento de la competencia.

En cualquier caso y a pesar de las buenas intenciones del GDPR, no parece del todo realista un cambio drástico en estas cuestiones pues, si bien es cierto que la nueva normativa introduce más obligaciones a los encargados y responsables del tratamiento de datos -bajo pena de sanción- así como reconoce más derechos para los interesados, no parece que cuente con el respaldo de las empresas tecnológicas y las corporaciones del Big data, nada dispuestas a renunciar al filón de negocio que supone hoy en día la privacidad. Una auténtica transformación del modelo, necesitaría forzosamente contar con la complicidad de aquellos que diseñan productos y ofrecen servicios relacionados para que tomen consciencia de los retos actuales y actúen en consonancia para la protección de los derechos y libertades de los ciudadanos, a quienes se les ofrezca productos y servicios respetuosos con su privacidad y por defecto.

IV. EL DERECHO AL OLVIDO DIGITAL.

1. Escenario previo.

La innovación tecnológica, junto con Internet, constituye ya una realidad imparable que en poco tiempo ha modificado nuestra forma de entender y vivir la vida y de relacionarnos con los demás. Este nuevo escenario ha supuesto enormes ventajas y facilidades para el día a día, pero, ciertamente, ha venido aparejado de nuevas vulneraciones para los derechos fundamentales.

La proliferación de datos personales que ocasionan las tecnologías del Big Data, así como la memoria virtual y permanente que conforman los motores de búsqueda online, suponen un almacenamiento, procesamiento y transferencia de información personal que, en ocasiones, vulnera derechos como la intimidad o el honor.

La digitalización masiva de la información y su almacenamiento son ahora la regla general y por defecto y ello, junto con la jurisdiccional mundial que se desprende del mismo concepto de Internet, han hecho costoso y en ocasiones hasta imposible, un ejercicio óptimo de los derechos de acceso, rectificación, cancelación y oposición.

La llamada era "post-privacy" obliga al Derecho a renovar sus mecanismos de protección y deviene necesario reformular conceptos jurídicos como "intimidad"

o "vida privada" cuyo significado se ha visto alterado, así como los mecanismos tradicionales de protección, que ahora resultan ineficaces.

Ante este nuevo panorama, se deben configurar nuevas construcciones jurídicas que refuercen el control sobre nuestros datos personales y consigan dotar de eficacia real los derechos de los ciudadanos. En ningún caso la innovación tecnológica puede usarse como pretexto para la vulneración de derechos y libertades fundamentales del mismo modo en que no puede asumirse sin más el mercadeo de información tan sensible como la que representa aspectos específicos del individuo.

Asimismo, los prestadores de contenidos online y de servicios de Internet deben cumplir con la normativa en materia de protección de datos, facilitar a los interesados el ejercicio de sus derechos y asumir responsabilidades por sus actuaciones corporativas que ocasionen perjuicios para los derechos humanos.

El derecho al olvido nace pues para combatir toda esta problemática, posibilitando no sólo los derechos de cancelación y oposición en Internet sino que, además, permite a los interesados el cifrado y borrado online de sus datos personales cuando éstos sean perjudiciales para los derechos fundamentales como la dignidad o la intimidad.

A grandes rasgos, podemos decir que el derecho al olvido tiene como finalidad proteger la privacidad de las personas frente a los retos que han propiciado la aparición de las nuevas tecnologías en connivencia con Internet. Es la respuesta que se ofrece desde el Derecho a los usuarios de Internet para que éstos puedan suprimir cualquier información personal por el que se vea afectada su privacidad, logrando una protección efectiva del derecho a la protección de datos lo que, a su vez, evita prácticas discriminatorias en torno a éstos.

2. La gestación del derecho al olvido por el TJUE.

El derecho al olvido, hasta hace poco de mera creación jurisprudencial, surge como respuesta a las reiteradas vulneraciones a la privacidad que los ciudadanos venían sufriendo en el entorno de Internet, manifestadas a consecuencia de la invasión que las novedades tecnológicas y el Big data han provocado en los derechos fundamentales.

A raíz de este nuevo escenario surgió el derecho al olvido, como respuesta lógica del Derecho frente a las vulneraciones de los derechos de los ciudadanos y gracias a pronunciamientos jurisprudenciales valientes y modernos, coherentes con los nuevos tiempos.

Las interpretaciones doctrinales y jurisprudenciales que hicieron emerger este nuevo derecho, giraron en torno al derecho a la protección de datos, noción consolidada en nuestra tradición jurídica cuyo reconocimiento se extiende por la inmensa mayoría de legislaciones nacionales de nuestro entorno, así como en el marco europeo, de igual modo que el derecho a la intimidad, al honor y a la dignidad.

Así las cosas, el Tribunal de Justicia de la Unión Europea reconoció, en su famosa sentencia de 13 de mayo de 2014 (Google Inc. v. Agencia Española de Protección de Datos[14]), más conocida como "caso Google" –cuyo contenido no se reproduce aquí por ser de sobra conocido-, la existencia de un derecho al borrado de nuestra información en Internet. Y con ello, se articulaba lo que se venía defendiendo desde hacía mucho tiempo por la doctrina: la protección de los derechos fundamentales no puede quedar supeditada a las restricciones tecnológicas.

Analizando el supuesto de hecho, el TJUE afirmó rotundamente que el tratamiento de datos personales por los buscadores en Internet puede afectar a los derechos fundamentales de las personas relativos al respeto de la vida familiar y de protección de los datos personales de forma significativa, cuando la búsqueda se lleva a cabo a partir del nombre de una persona física, pues ello permite al internauta hacerse una configuración apriorística de una persona en base a la lista de resultados ofrecidos.

Como en el caso en concreto la información ofrecida por el buscador era lícita y veraz, el Tribunal estimó que, incluso en estos casos, ésta puede resultar desproporcionada y, en consecuencia, provocar una intromisión ilegítima en los derechos del afectado. Así, dispuso que un tratamiento de datos puede devenir incompatible con el Derecho, no sólo cuando los datos sean inexactos sino también cuando éstos 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.

Es decir, incluso tratándose de datos o informaciones exactas, verídicas o lícitas, podría considerarse su uso como inadecuado lo que obligaría al motor de búsqueda a eliminar de los resultados tal información puesto que el tratamiento de datos debe ser legítimo durante todo el periodo en que se lleve a cabo.

En cuanto a la responsabilidad en el tratamiento de este tipo de datos, el pronunciamiento del TJUE entraña también novedades y es que extendió a los

14 Sentencia del TJUE de 13 de mayo de 2014, asunto C-131/12, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja*.

gestores de los buscadores de Internet dicha responsabilidad, 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 permitirá a los particulares dirigirse directamente ante los buscadores en Internet para ejercer los derechos de rectificación y oposición de sus datos.

De esta forma, el Tribunal por una parte, se avanza a lo dispuesto después por el RGPD en cuanto a la aplicación territorial de la normativa europea, sometiendo a la legislación no sólo a los actores europeos sino también a todos aquellos que desempeñen su actividad en su territorio y, por otra parte, extiende la aplicación de la normativa de protección de datos a los motores de búsqueda en tanto que almacenan, indexan y ponen a disposición del público información publicada por terceras personas.

La relevancia jurisprudencial de esta resolución debe entenderse desde una óptica garantista y la necesidad de hacer evolucionar el Derecho al mismo compás que la sociedad. En un momento en que la desconexión tecnológica parece ya imposible, deben darse respuestas jurídicas a los problemas que ocasionan las nuevas herramientas tecnológicas respecto de los derechos y las libertades de sobra consolidados.

3. El derecho de supresión en el GDPR.

Como ya se ha hecho mención, una de las principales novedades introducidas por el Reglamento europeo de protección de datos es la incorporación, por vez primera y expresamente, del derecho al olvido o, en su denominación definitiva, el derecho de supresión.

Así, el artículo 17 del GDPR configura el derecho al olvido tal y como había reparado el TJUE en el ya famoso caso Google v. España, configurándolo como una suerte de derivación del derecho a la intimidad y propia imagen, y como extensión del derecho al honor.

Podría definirse el derecho al olvido como el derecho al borrado digital de hechos pasados que tiene toda persona que se haya sentido vulnerada en un derecho fundamental, debido a causas justificadas o porque con el paso del tiempo sus datos han perdido su virtualidad. El artículo 17, por su parte, lo define como el "derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales" cuando concurran ciertas circunstancias.

No debe confundirse el derecho al olvido como el derecho a configurar un pasado a medida, obligando a los editores de páginas web o a los motores de búsqueda a suprimir aquellos resultados o contenidos digitales que no quieran verse asociados a una persona –nombres y apellidos-, pero sí que supone un límite a la memoria eterna de Internet, dónde el tiempo es lineal y no se distingue entre pasado y presente lo que provoca en muchos casos, bien por el transcurso del tiempo, bien por la descontextualización, una vulneración de los derechos fundamentales del afectado, pudiendo perjudicar seriamente el libre desarrollo de su personalidad y hasta su dignidad personal.

Para evitar malinterpretaciones, debe examinarse el derecho al olvido junto con el "habeas data", el derecho a la protección de datos desde la perspectiva de la potestad del interesado a tener un control sobre sus datos, a la autodeterminación informativa. En definitiva, como extensión de los derechos ARCO, especialmente relacionado con el derecho de cancelación y oposición de los datos personales en el ámbito de Internet, conceptos aceptados comúnmente por la legislación, doctrina y jurisprudencia y que ahora ostentan una nueva virtualidad gracias a las nuevas herramientas tecnológicas que han permitido nuevas formas de atentar contra bienes jurídicos protegidos de sobra ya consolidados, como son el derecho al honor o a la intimidad.

Este punto de vista parece compartirse por el legislador europeo que en el RGPD no parece considerar el derecho al olvido como un derecho autónomo o diferenciado de los derechos ARCO, sino como una consecuencia de los mismos. De esta forma, puede definirse el derecho de supresión como la potestad otorgada a los ciudadanos para reclamar que sus datos desaparezcan de Internet cuando puedan afectar al libre desarrollo de ciertos derechos fundamentales.

Se incorpora así, a las potestades existentes de solicitar y obtener de los responsables de los ficheros, que determinados datos sean suprimidos cuando, entre otros casos, se hayan obtenido de manera ilícita, cuando se haya retirado el consentimiento prestado, cuando estos ya no sean necesarios para la finalidad para la que fueron recogidos o cuando el interesado se oponga al tratamiento, todo ello en el entorno digital.

Es de aplicación pues la doctrina existente en esta materia, que ha habido de adaptarse a los nuevos marcos sociales y tiempos de la técnica. Decía ya Díez Picazo[15] en el año 1979, cuando aún ni se atisbaba la revolución digital de lo que sería Internet, que la publicación de la biografía de una persona todavía viva exige su consentimiento y por ello, debe exigirlo también cualquier investigación sobre

15 Díez-Picazo, L.: *Derecho y masificación social. Tecnología y Derecho privado (dos esbozos)*, Civitas, Madrid, 1979, p. 114.

su vida anterior, el apoderamiento de sus datos y el archivo de los mismos. Del mismo modo, es posible encontrar referencias al derecho al olvido hace ya 30 años de la mano de Salvador Coderch[16] que reflexionaba acerca de los límites de la memoria pública colectiva sobre la intromisión a la intimidad, a propósito del comentario de la famosa sentencia *Sidis v. F. R. Publishing Corp*[17].

El GDPR pues, de algún modo moderniza los derechos tradicionales para lidiar con el nuevo marco social, cultural y tecnológico en el que se insertan. Esto queda patente, por ejemplo, cuando prevé que el derecho de rectificación se pueda ejercitar a posteriori especialmente cuando el interesado prestó su consentimiento siendo un niño y se quiere suprimir datos de Internet (considerando 65), cuestión plenamente contextualizada con el comportamiento de los adolescentes de hoy en día.

En cuanto a su naturaleza jurídica, si bien es cierto que el derecho al olvido tiene su origen en el derecho a la intimidad y a la protección de datos, éste tiene sus raíces indudablemente en la dignidad del ser humano y el desarrollo de su personalidad. El RGPD, en consecuencia, vincula el derecho al olvido con el derecho al control del interesado sobre sus propios datos cuando obliga a los responsables a indicar a los sujetos objeto de tratamiento la situación del mismo, así como los cambios que se produzcan para que éstos puedan tomar la decisión más acertada en cuanto a sus datos personales; queda patente así el cambio de modelo del que antes hablábamos que considera el "habeas data" como un principio inspirador de toda la legislación.

A fin de reforzar tal extremo, el derecho de supresión obliga al responsable del tratamiento que haya hecho públicos datos personales a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos o las copias o réplicas de tales datos. Y al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las posibilidades técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales (párrafo segundo del artículo 17).

Ahora bien, el derecho al olvido no es absoluto, exige una ponderación con los derechos con los que entra en conflicto lo que obliga a un examen pormenorizado del caso concreto para lograr el equilibrio entre derechos que se superponen. La normativa europea también es consciente acerca de los límites de este derecho y establece como tales el derecho a la libertad de expresión e información, razones

16 Salvador Coderch, P.: ¿Qué es difamar? Libelo contra la Ley del Libelo, Civitas, Madrid, 1987, p. 98.

17 U.S. Court of Appeal for the Second Circuit - 113 F. 2d 806 (2d Cir. 1940), 22 de julio de 1940.

de interés público, fines de investigación o estadístico, el cumplimiento de una obligación legal o el derecho de reclamación (párrafo tercero del artículo 17).

Así pues, el derecho de supresión puede ser limitado por otros derechos con los que puede entrar en conflicto lo que exige, una vez constatado la existencia de una colisión entre ellos, examinar la intensidad y trascendencia con la que cada uno de éstos resultará afectado, conforme al contexto concreto y teniendo en cuenta que las reglas jurisdiccionales clásicas no pueden servir como fundamento único en esta ponderación pues Internet tiene unas pautas de funcionamiento que alteran las reglas de juego preexistentes y que obligan a examinar los casos nuevamente. Así, por ejemplo, frente a una colisión frente a la libertad de información y el derecho al olvido, no es conveniente aplicar la doctrina del Tribunal Constitucional en la materia pues, puede tratarse de una información lícita, veraz y de tratamiento neutro y aun así atentar contra los derechos fundamentales de una persona[18].

Por último, y planteándose retos de futuro cabría reflexionar sobre el ejercicio del derecho al olvido en el entorno digital donde son las personas físicas que deben ejercitarlo frente a personas jurídicas que se encuentra muchas veces en distintas jurisdicciones, con trabas procesales, lo que requiere de una dedicación personal y unos conocimientos jurídicos que no son exigibles a todo ciudadano, y aún menos cuando de ello depende la vulneración de sus derechos fundamentales. Por ello, un paso más allá y sin duda deseable sería lograr el borrado automático de ciertos datos personales en la Red, sin necesidad de que el propio interesado tenga que dar ningún paso para obtener dicho resultado, sino que bastase con establecer plazos automáticos de caducidad.

Esta propuesta encajaría dentro de lo que se ha venido llamando *"privacy by design"*, es decir, la introducción, mediante políticas públicas y prácticas empresariales, de un estándar de privacidad desde el diseño y por defecto, de forma que los usuarios o interesados no tengan que actuar proactivamente para exigir el cumplimiento de sus derechos fundamentales, sino que tanto la tecnología como las prácticas corporativas sean respetuosos ab initio con la privacidad de los ciudadanos[19].

18 Ocurrió así en el mencionado caso Google donde, mediante la introducción en el motor de búsqueda de un nombre y apellidos, se facilitaba como primeros resultados una serie de información verídica y legal acerca del embargo de ciertos bienes de la persona en cuestión, ocurrido años atrás. El Tribunal de Justicia de la Unión Europea entendió que debía reconocérsele al afectado un derecho al olvido digital puesto que tal resultado en el buscador, dada la descontextualización y el transcurso del tiempo, producían un daño en la credibilidad profesional del demandante y en su honor.

19 Por ejemplo, en relación a los cookies, el Prof. Ureña propone adoptar una normativa que obligue por defecto a que los software de navegación estén configurados para el rechazo de los cookies, de manera que quién quisiera admitirlos debería reconfigurar su navegador en sentido contrario, justo lo contrario de lo que ocurre ahora, "de este modo, la Administración verificaría que todos los software de navegación que se fabrican, comercializan o importan, cumplen con el requisito que con carácter obligatorio aquélla ha impuesto".

El GDPR ha abierto la puerta a esta posibilidad, expresamente su artículo 25 cuando contempla la introducción de medidas de privacidad desde el diseño, y a lo largo de su articulado lo presenta como un principio inspirador de toda la normativa de protección de datos siempre que sea posible "teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas públicas". Todo ello aparejado a otras medidas de minimización de tratamiento de datos u otras garantías para la preservación de la privacidad como las técnicas de pseudonimización.

Así pues, se trataría de instaurar el derecho al olvido como una regla general, actuando de forma automática, por defecto y no sólo bajo petición[20], sin perjuicio de su examen pormenorizado en aquellos casos en los que resulte evidente una colisión de derechos fundamentales.

V. CONCLUSIONES.

Todos los sistemas jurídicos están condicionados por un determinado nivel de conocimientos científicos y de técnicas interpretativas que se ponen a prueba cuando, por ejemplo, algún avance científico-técnico requiere de una adecuada respuesta del ordenamiento jurídico, momento en el que se evidencia su flexibilidad para adaptarse a un nuevo contexto.

El entorno cuotidiano actual ha puesto en jaque los parámetros a los que la privacidad venía acostumbrada, ocasionando nuevas formas de lesión para los derechos de la personalidad. Las nuevas herramientas tecnológicas junto con el proceder de Internet, las corporaciones del Big data y las nuevas pautas de comportamiento, comunicación y consumo, han hecho patente un cambio necesario de legislación capaz de proteger los derechos fundamentales de los ciudadanos.

Inevitablemente las transformaciones técnicas y científicas tienen el correspondiente influjo en el ordenamiento jurídico que debe adaptarse mediante interpretaciones extensivas o bien dictando nuevas regulaciones, debiendo existir en todo caso una correlación entre el avance científico-técnico y el cambio jurídico que éste exige, pues la proyección social de ambos es ciertamente indiscutible.

Ureña Salcedo, J. A.: "Internet y la protección de datos personales" en AA. VV.: *Monografías de la Revista Aragonesa de Administración Pública* (coord. Por A. Cayón Galiardo), Diputación General de Aragón, vol. IV, Zaragoza, 2001, p.134.

20 De Terewagne, C.: "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", *Revista d'Internet, Dret i Política (IDP)*, 2012, núm. 13°, pp. 53-65.

En este escenario de evidente pérdida de privacidad, los Estados han tratado de orientar sus legislaciones hacia una mayor cobertura de las garantías personales, pero, ya sea por los tiempos del legislador o bien por la constante renovación de las tecnologías y expansión de Internet, los mecanismos previstos hasta ahora no se han revelado como enteramente eficaces.

Así, han sido los tribunales nacionales e internacionales quienes han jugado un papel imprescindible para la protección de la privacidad y en el amparo de las garantías ciudadanas, aunque con notables dificultades procesales, derivadas principalmente de problemas de jurisdicción así como de impedimentos tecnológicos.

La actuación de la jurisprudencia del TJUE ha sido definitiva, capaz de dar una respuesta adecuada ante los riesgos existentes para la protección de ciertos derechos fundamentales en la era de Internet. La creación jurisprudencial del derecho al olvido, a través de derechos como la privacidad y la personalidad, es una buena muestra de ello, evitando las vulneraciones que de manera reiterada venían sucediéndose por grandes corporaciones acostumbradas a tratar a los datos personales como un producto comercializable. Esta coyuntura tiene una repercusión mayor en el ámbito digital, donde la memoria electrónica eterna y las acciones de compilación que llevan a cabo los buscadores de Internet hacen de estas vulneraciones un auténtico calvario.

Sin embargo, las circunstancias actuales exigen un cambio sustancial del modelo capaz de poner límite a las nuevas herramientas tecnológicas resultando a la vez efectivo para la protección de los derechos fundamentales de los ciudadanos. Con el nuevo Reglamento europeo de Protección de Datos, se pretende dar un giro en esta materia, otorgando a los ciudadanos un mayor control sobre su información personal e introduciendo medidas desde el diseño para la protección de los derechos fundamentales por defecto.

La nueva normativa, trata de poner fin al principio de territorialidad que tanto dificultaba la garantía de los derechos en materia de privacidad, disponiendo su aplicación no sólo a los responsables o encargados del tratamiento de datos establecidos en la Unión Europea sino también a aquéllos que, sin estar domiciliados en ella, lleven a cabo acciones de tratamiento de datos en suelo europeo. Del mismo modo, con su formulación expresa del derecho al olvido, faculta a los ciudadanos la posibilidad de borrar digitalmente aquella información que vulnere derechos fundamentales como la intimidad o el honor.

En definitiva, se trata de establecer las bases para que el avance tecnológico no suponga un retroceso en la protección jurídica de los ciudadanos, sino que sea un presupuesto para configurar nuevos mecanismos jurídicos capaces de mantener

intacto el núcleo duro de protección de tales derechos, pues la función social que caracteriza al Derecho le obliga a dar solución a los nuevos conflictos que en ella se suscitan y así dotar de seguridad jurídica a los ciudadanos.

Así lo ha afirmado el TJUE disponiendo que las limitaciones de las nuevas tecnologías no pueden ser una excusa para las intromisiones ilegítimas en los derechos fundamentales de los ciudadanos en Internet, que deben protegerse por encima de cualquier circunstancia.

Si bien es cierto que con el GDPR se han materializado grandes esfuerzos para acabar con la desprotección actual, habrá que esperar un tiempo para ver los efectos de su entrada en vigor así como la armonización definitiva de las legislaciones nacionales en este sentido, pues puede pensarse a priori, que se necesitarán muchos más esfuerzos legislativos así como el compromiso por parte de Estados y corporaciones del Big data para llevar a cabo un verdadero cambio del modelo y frenar de manera efectiva la expropiación de la privacidad a la que estamos actualmente sometidos.

Es necesaria una actitud reflexiva, crítica y consciente de la nueva coyuntura social, tecnológica, económica y jurídica a escala global, lo que se ha llamado por algunos "responsabilidad tecnológica"[21]. Las necesidades humanas están en continua evolución y no resultan impermeables a las innovaciones tecnológicas, por ende, la teoría y la práctica de la democracia no puede resultar insensible a este nuevo escenario pues los principios sobre los que se asienta el ordenamiento jurídico permanecen inmutables y deben respetarse con independencia del medio en el cual se apliquen. *Ubi societas ubi ius*.

21 Pérez Luño, A. E.; *Los derechos humanos*, Universitas, cit., p. 42.

BIBLIOGRAFÍA

Bauman, Z.: *Modernidad líquida*, Fondo de Cultura Económica, México, 2000.

Berrocal Lanzarot, A. I.: *Derecho de supresión de datos o derecho al olvido*, Reus, Madrid, 2017.

De Terewagne, C.: "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido", *Revista d'Internet, Dret i Política (IDP)*, 2012, núm. 13º.

Díez-Picazo, *L.: Derecho y masificación social. Tecnología y Derecho privado (dos esbozos),* Civitas, Madrid, 1979.

Frosini, V.: *Cibernética, derecho y sociedad,* Tecnos, Madrid, 1982.

Gudín Rodríguez-Magariños, F.: *Nuevo Reglamento Europeo de Protección de Datos versus Big Data,* Tirant lo Blanch, València, 2018.

Newman, A. L.: *Data privacy and the global economy,* Cornell University Press, New York, 2008.

Pérez Luño, A. E.: *Los derechos humanos en la sociedad tecnológica, Universitas, Madrid, 2012.*

Salvador Coderch, P.: *¿Qué es difamar? Libelo contra la Ley del Libelo,* Civitas, Madrid, 1987.

Solove, D. J.; *The future of reputation*, Yale University Press, New Haven and London, 2007.

Troncoso Reigada, A.: *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, València, 2008.

Ureña Salcedo, J. A.: "Internet y la protección de datos personales" en AA. VV.: *Monografías de la Revista Aragonesa de Administración Pública* (coord. Por A. Cayón Galiardo), Diputación General de Aragón, vol. IV, Zaragoza, 2001.