CEFD
Cuadernos Electrónicos de Filosofía del Derecho

ACTAS I CONGRESO INTERNACIONAL 70 ANIVERSARIO DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS

Internet, Big data y nuevas tecnologías: repercusiones y respuestas del ordenamiento jurídico

Internet, Big data and new tecnologies: implications and responses from the legal system

Marina Sancho López
Universidad Internacional de Valencia

RESUMEN.

Cada uno de los movimientos que se suceden en la red genera información que se digitaliza en código binario y se almacena masivamente. La arbitrariedad con la que operan las grandes corporaciones del Big data así como la opacidad de los algoritmos empleados por la inteligencia artificial han dado origen a nuevas formas de vulneración de derechos, dónde la intimidad y el honor han resultado los primeros damnificados. Este escenario requiere un replanteamiento de conceptos jurídicos como estado o vida privada que han cobrado nuevos significados y demandan construcciones jurídicas capaces de reforzar el control sobre nuestros derechos más fundamentales.

PALABRAS CLAVE.

Privacidad, Internet, Protección de datos, derechos fundamentales.

ABSTRACT.

Each of the movements that occur in the network generates information that is digitized in binary code and it is stored massively. The arbitrariness with which the Big Data corporations operate as well as the opacity of the algorithms used by artificial intelligence have given rise to new forms of violation of rights, where intimacy and honour have been the first victims. This scenario requires a rethinking of legal concepts such as state or private life that have taken a new meanings and, therefore, they demand legal constructions capable of reinforcing control over our most fundamental rights.

KEY WORDS.

Privacy, Internet, Data Protection, fundamental rights.

Sumario: 1. El nuevo escenario derivado de la modernidad líquida. 2. El *Big data* y la influencia de los algoritmos en los derechos y libertades. 3. *Dataveillance*, exclusión y segmentación social en el *Big data*. 4. La privacidad como mercancía: el negocio de los datos personales. 5. Reflexiones finales. 6. Referencias bibliográficas.

1. El nuevo escenario derivado de la modernidad líquida

Cada cierto tiempo, se producen determinados fenómenos sociales que suponen un cambio de paradigma sustancial en las prácticas políticas, económicas, sociales, o incluso culturales, propias de un determinado contexto espacio-temporal. Vivimos en un momento de cambio constante, donde la técnica no se detiene y dónde la distracción de un solo pestañeo puede alejarte de la vanguardia; usando la terminología de BAUMAN, es ésta una época de "modernidad líquida"[1]. En este sentido, la revolución tecnológica y digital aparejada a la Sociedad de la Información, ha venido a redefinir amplios espacios de la vida en comunidad, y a variar continuamente las formas de interacción social propias de nuestro momento histórico. En la *posmodernidad* actual, el *Big data* supone una de las manifestaciones más intensas de un nuevo paradigma, donde conceptos jurídicos que tradicionalmente no presentaban mayores discusiones, como por ejemplo los de intimidad o vida privada, requieren de un proceso de reflexión para adaptar sus proposiciones al nuevo estado de cosas.

Esta nueva coyuntura reclama de la Ciencia, el Derecho, la Ética, la Economía y la Política, una "responsabilidad tecnológica", es decir, una actitud reflexiva, crítica y consciente de los nuevos problemas que, en las diversas esferas de la vida suscita la tecnología y a los cuales la sociedad y, particularmente el ordenamiento jurídico, no pueden ignorar[2]. La necesaria evolución de la colectividad no puede restar un ápice del contenido garantista que requiere la protección de los derechos fundamentales en un Estado social y democrático de Derecho, que debe adoptar las precauciones

[1] Cfr. BAUMAN . *Modernidad líquida*, Fondo de Cultura Económica, Madrid, 2017.

[2] PÉREZ LUÑO/GONZÁLEZ-TABLAS. "Ciberciudadanía y teledemocracia", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro II, Dykinson, Madrid, 2013, p. 1113.

necesarias así como accionar los mecanismos indispensables para lograr un progreso tecnológico y social compatible con el respeto a esos derechos fundamentales[3].

2. El *Big data* y la influencia de los algoritmos en los derechos y libertades

Llamamos *Big data* al almacenamiento, tratamiento y transferencia de datos a gran escala a través de las tecnologías de Internet. En la globalización del siglo XXI, las innovaciones tecnológicas junto con el nuevo modelo económico y social, han hecho proliferar enormes cantidades de bases de datos relativos a realidades tangibles (datos físicos) o intangibles *a priori* pero convertidos mediante algoritmos en información digital. Entre los unos y los otros hay un número descomunal de datos de carácter personal. La relevancia de estos datos masivos no sólo afecta a cuestiones directa e indirectamente vinculadas a nuestra privacidad, sino que tiene una trascendencia que abarca la propia configuración del tejido social.

Como señalan MAYER-SCHÖNBERGER y CUKIER, "la era de los datos masivos pone en cuestión la forma en que vivimos e interactuamos con el mundo. Y aún más, la sociedad tendrá que desprenderse de parte de su obsesión por la causalidad a cambio de meras correlaciones: ya no sabremos por qué, sino solo qué. Esto da al traste con las prácticas establecidas durante siglos y choca con nuestra comprensión más elemental acerca de cómo tomar decisiones y aprehender la realidad"[4].

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 de explotarlos posteriormente, por ejemplo, para fines publicitarios–[5]. Estos datos y metadatos se consiguen, generalmente, a través de las aplicaciones que descargamos en nuestros dispositivos inteligentes que cada vez exigen con más frecuencia acceso a

[3] Como bien señala DÍEZ-PICAZO, la experiencia histórica nos ha enseñado que el Derecho, como fenómeno en sí mismo considerado, es ante todo "un proceso de cambio y de progreso jurídico". Cfr. *Experiencias jurídicas y teoría del Derecho*, Ariel, Barcelona, 1983, p. 300.

[4] Cfr. *Big data. La revolución de los datos masivos*, Turner, Madrid, 2015, p. 18.

[5] Así, si un teléfono móvil tradicional tenía información sobre a quién llamábamos y de cuántos SMS enviábamos al mes, un Smartphone sabe 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, en qué noticias estamos más interesados…hasta el punto de poder hacerse una configuración de nosotros a imagen de patrones de comportamiento –que muchas veces no tiene por qué coincidir con la verdadera–, como por ejemplo el nivel adquisitivo de una persona, o su entorno social.

información personal para proceder a la instalación[6]. Piénsese, por ejemplo, en los permisos para acceder a la geolocalización del dispositivo resultantes de la aceptación en bloque de las condiciones de uso de dichas aplicaciones. En la medida en que los propios hábitos de búsqueda del usuario a través de sus dispositivos están a disposición de las empresas privadas, si a esto le sumamos la posibilidad de acceder a los datos de geolocalización en todo momento, ello permite, por ejemplo, introducir una publicidad personalizada allá donde esté o, aún más inquietante, allá dónde se prevea vaya a estar una persona, algo que ya hemos comprobado en nuestras búsquedas o visitas a sitios de Internet.

Estos bancos de datos contienen información relativa a nuestra identidad (nombres, lugar de residencia, profesión, estado civil, propiedades…) así como otra información personal tan diversa como nuestra religión, ideología, clase social, salud… La información, en el primer caso, se obtiene de registros públicos o privados y por ello podíamos decir que es "real" mientras que, en el segundo caso, ésta es obtenida a través de otros parámetros -no siempre fiables- como nuestras pautas de comportamiento, preferencias culturales o patrones de consumo. Podría aquí diferenciarse entre los datos estructurados, aquellos que provienen de fuentes de información conocidas y que, por a tanto, son fáciles de medir y analizar en los sistemas tradicionales, en contraposición a lo que se ha dado en llamar datos no estructurados. Para que sea posible analizar estos últimos, teniendo en cuenta la variedad de su origen, así como la rapidez con que se incrementa su volumen, ha sido necesario el desarrollo de nuevos modelos de software para adecuarse a su carácter disperso y heterogéneo[7].

Los distintos 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. Como se

[6] Sobre esta cuestión, HARCOURT señala la construcción de perfiles comerciales elaborados por Google a través del estudio de los correos electrónicos de sus usuarios de Gmail, lo que el autor norteamericano ha denominado como "conocimiento digital" (*digital knowledge*). La construcción del perfil mediante la monitorización de las palabras escritas en los correos, los archivos adjuntos, el contenido de las páginas web visitadas por el usuario de Gmail, así como toda la información demográfica obtenida en el momento de crear la cuenta permite a Google obtener un retrato robot del consumidor, pudiendo así incidir en sus hábitos comerciales, o lo que eufemísticamente denomina el autor norteamericano: "hacer la experiencia online más personal y disfrutable para el usuario/consumidor". Cfr. "Governing, Exchanging, Securing: Big Data and the production of a digital knowledge", *Public Law and Legal Theory Working Paper Group*, Columbia Law School, 2014, pp. 4-5.

[7] Cfr. PUYOL MORENO. "Una aproximación a Big Data", *Revista de Derecho, UNED*, nº 14, 2004, p. 483.

verá a continuación, esta es una de las vertientes más interesantes del nuevo contexto resultante del *Big data*, en tanto que supone un nuevo paradigma en los itinerarios de evolución del control social formal.

Pero no sólo se trata de acumular datos, sino de interrelacionarlos entre sí para lograr aumentar exponencialmente la información a obtener y, de ese modo, sacarle un mayor partido. Es lo que SOLOVE llama *agregación*[8]: conformar el perfil de una persona a través de la triangulación y organización de la información que se ha obtenido sobre ella, generando nuevos datos sobre un individuo. Contar con estos nuevos datos resulta especialmente útil para el desarrollo de determinadas campañas publicitarias que se elaboran a partir de este proceso de *agregación*. Sin embargo, dicho proceso, al alterar las expectativas de las personas, supone una amenaza para la libertad personal y la intimidad, ya que el sujeto no ostenta control alguno sobre el conocimiento que se está obteniendo a través de su información personal a la vez que se influye negativamente en la capacidad crítica de los individuos[9].

Como se ha dicho, Internet ha logrado aumentar exponencialmente el tráfico de información y, a través de la interconexión mundial de bases de datos y la cantidad de copias de las mismas, puede afirmarse que el aumento de tráfico de información que discurre por esta vía, es hoy en día imparable[10]. Esto en sí mismo no es negativo, gracias a ello tenemos acceso a una cantidad enorme de fuentes de casi cualquier parte del mundo que de otro modo sería impensable alcanzar. ¿Cual es la otra cara de la moneda? La afectación de los derechos fundamentales de la ciudadanía.

Por lo tanto, puede reconocerse que el *Big data* supone un cambio tanto cuantitativo como cualitativo en los estándares de riesgo que los derechos fundamentales podían tradicionalmente asumir con el surgimiento de Internet como vehículo de información y comunicación masivo. Hablamos de

[8] Cfr. SOLOVE. "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol. 154, nº 13, pp. 477 ss.

[9] Como expone O'NEIL, "nos clasifican y categorizan y nos asignan puntuaciones en cientos de modelos en base a los patrones y preferencias que hemos desvelado. Y esto constituye un poderoso fundamento para muchas campañas publicitarias legítimas, aunque también alimenta a la publicidad depredadora: los anuncios que identifican a las personas con grandes necesidades y les venden promesas falsas o productos a precios excesivos". Cfr. *Armas de destrucción masiva. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, Madrid, 2018, p. 89.

[10] Así, MORENO MUÑOZ apunta cómo "datificación, internet de las cosas y *big data* convergen sobre una base común de herramientas, tecnologías y procesos a gran escala que consolidan una tendencia a definir el modo en que las organizaciones o empresas tradicionales prestan sus servicios, entendidos en el nuevo contexto tecnológico como actividades dependientes de una infraestructura global de datos, de la que se extraen conocimiento e información para desarrollar procesos críticos de su negocio, adoptar decisiones estratégicas y responder a la evolución de la competencia con un mejor control de los datos relevantes para su actividad". Cfr. "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", *Dilemata,* nº 24, 2017, p. 9.

modificación cuantitativa porque aumenta la intensidad de los riesgos, siendo asimismo el nuevo paradigma de distinta percepción cualitativa en tanto que la propia naturaleza de estos riesgos se ha visto modificada.

Sobre esta cuestión, la nueva perspectiva axiológica parte de la necesidad de proteger los derechos fundamentales del ciudadano, no únicamente respecto de los terceros que pudieran invadir su esfera personal, sino también en relación con la posible explotación mercantil de los datos personales por entidades especializadas en estas prácticas[11], e incluso ante la necesaria protección de la privacidad que, paradójicamente, supone la constante y voluntaria exposición de nuestra vida privada en las redes sociales. Desde esta óptica, no es descabellado afirmar que las dinámicas propias del *Big data* han supuesto una redefinición de los procesos sociales sin precedentes.

3. *Dataveillance*, exclusión y segmentación social en el *Big data*

Toda dinámica de transformación social viene asociada a una serie de prácticas que determinan el nuevo estado de cosas a nivel político, económico e incluso cultural, resultantes del cambio histórico. El concepto *dataveillance* ha sido acuñado por CLARKE para hacer referencia al uso sistémico de los procedimientos de tratamiento y análisis de datos masivos, con la finalidad de investigar o monitorizar las dinámicas de actuación o interacción social[12]. En este sentido, el tratamiento de datos masivos, así como la preeminencia de las redes sociales en los procesos de comunicación social suponen un nuevo escenario al que han sabido adaptarse los sistemas de vigilancia y disciplina (*surveillance*) emanados del *Big data* (de ahí la adecuación del término *dataveillance*).

Siguiendo esta línea argumentativa, el filósofo surcoreano BYUNG-CHUL HAN, partiendo de las premisas asentadas por BENTHAM y FOUCAULT sobre el control social[13] y revisitándolas en el contexto del *Big data*, ha desarrollado el concepto de *panóptico digital* como práctica que consolida el

[11] Los *Data Brokers* son empresas que se encargan directamente de hacer negocio con la privacidad, son vendedores de información que se dedican a recolectar datos de los consumidores (la mayoría de veces sin su consentimiento) y vendérselos a un tercero. Pese a que este mercadeo es opaco y actúan encubiertos en el anonimato, se calcula que estas empresas no llegan ni a la decena pero, sin embargo, controlan todo el tráfico de Internet.

[12] Cfr. *Introduction to Dataveillance and Information Privacy*, Australian National University, 2006.

Vid. BENTHAM. *Panóptico,* Círculo de Bellas Artes, Madrid, 2011; FOUCAULT. *Vigilar y castigar. Nacimiento de la prisión*, Siglo XXI, Madrid, 2009.

control social en las redes sociales como nuevo paradigma de vigilancia[14]. Desde la *sociedad de la transparencia* descrita por HAN se transita fácilmente a lo que se ha denominado como *sociedad de la exposición*[15]. En ésta, se reconoce la necesidad que sienten las personas por exponerse, no sólo inducidos por el fetichismo digital impuesto por las redes sociales, sino porque representa la única forma de existir, de proyectarse en el medio social. De este modo, cada sujeto es su propio objeto de publicidad, todo se mide en su valor de exposición[16].

Igualmente, deben considerarse los riesgos que suponen para la cohesión social las posibles prácticas discriminatorias que puedan derivarse de la ideología del algoritmo que orienta el *Big data*. En este sentido, la posible exclusión de colectivos e individuos dentro de este nuevo paradigma, así como las limitaciones en el disfrute de derechos y libertades públicas pueden derivar en un proceso de segmentación social donde los presupuestos estructurales de un Estado democrático de Derecho puedan verse socavados.

Y es que, no puede calificarse el *Big data*, ni tampoco el proceso técnico seguido para el análisis y tratamiento de datos masivos como un fenómeno neutral o meramente científico. No puede servir como argumento legitimador el hecho de que una decisión esté basada en cálculos algorítmicos por su supuesto carácter científico, y en consecuencia pretendidamente neutral, en tanto que las variables utilizadas como muestras sobre las que inciden los algoritmos pueden responder a una serie de consideraciones motivadas por razonamientos de tipo político, económico o social. Si bien los algoritmos se atienen a una lógica científica-matemática, la forma en que éstos son proyectados al estudio de los procesos sociales responde indudablemente a unas coordenadas ideológicas concretas y, por tanto, existe cierto riesgo de que se produzca un proceso reduccionista y simplificador de etiquetaje respecto de determinados colectivos, a partir de prácticas discriminatorias de tipo social o económico que pueden determinar una segregación excluyente de los grupos afectados. La consumación usual de estos procesos da lugar, según ciertos autores, a la creación de una *sociedad de clases digital*[17].

[14] Cfr. *La sociedad de la transparencia*, Herder, Barcelona, 2013.

[15] HARCOURT. *Exposed. Desire and Disobedience in the Digital Age*, Harvard University Press, Cambridge, 2015.

[16] Cfr. *La sociedad de la transparencia*, ob. cit., p. 29.

[17] Cfr. HAN. *Psicopolítica*, Herder, Barcelona, 2014, p. 99.

Sobre esta cuestión, puede resultar pertinente el siguiente supuesto como ejemplo de discriminación social, en tanto que tiene por objeto algo tan cotidiano como el nombre de las personas. La página web francesa *Ton prenom*[18]*,* portal que sirve de enciclopedia para facilitar la elección del nombre de los recién nacidos, utiliza un algoritmo que discrimina en contra de ciertos nombres personales y a favor de otros. Los padres primerizos que quieren elegir el nombre para sus hijos pueden recurrir a sus servicios, pero habrán de tener en cuenta que el algoritmo de esta página asume por defecto que se desea evitar un nombre de origen árabe.

Como apunta MONASTERIO ASTOBIZA, "el algoritmo deja marcada por defecto la opción de *favorecer* un nombre de origen francés, marca por defecto la opción *indiferente* para los nombres de origen inglés o judío, pero marca la opción *evitar* para nombres de origen árabe"[19]. Como puede verse, este caso presenta de qué manera los algoritmos, si bien son un producto técnico-científico, pueden responder a una determinada opción ideológica que puede predeterminar su incidencia en los procesos sociales. En este sentido, la discriminación social producida por dicho algoritmo no sería asumible, en tanto que muestra de forma explícita un sesgo atendiendo a la procedencia étnica de los nombres.

Además de los casos de discriminación social, el *Big data* también puede incurrir en casos de discriminación económica, si bien en muchos de los supuestos existirá una correlación entre ambas categorías. Piénsese en las personas que viven en los *márgenes* del *Big data*, aquéllas que debido a causas diversas (pobreza, geografía, estilo de vida…), no son *datificados*, distorsionando a favor de las mayorías integradas en el sistema económico y social la orientación de la lógica algorítmica que orienta el tratamiento y análisis de los datos masivos[20].

Los casos de discriminación económica y social pueden llevar en casos extremos a la exclusión, a la creación de colectivos silenciados, en tanto que no se atiende a sus preferencias o comportamientos para la oferta de bienes y servicios por el Mercado e incluso, la atención y asistencia por parte de los poderes públicos. De acuerdo con SOLOVE, esta situación no sólo afecta al desarrollo del medio social, dado que supone una ruptura de las expectativas que determinados colectivos albergan en los

[18] http://tonprenom.com/bebe

[19] Cfr. "Ética algorítimica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", *Dilemata*, nº 24, 2017, p. 199.

[20] Cfr. LERMAN "Big data and its exclusions", *Stanford Law Review*, 66, 2013, p. 57.

poderes públicos, sino que "afecta a la estructura social en tanto que altera la confianza de la ciudadanía en las instituciones, suponiendo una situación de frustración y desamparo"[21].

Por otra parte, existen determinados espacios de participación pública asociados a la democracia representativa que pueden verse afectados por el *Big data,* pues resulta significativa la creciente importancia de los datos masivos en la planificación de las campañas electorales de los partidos políticos. Obviamente, la posibilidad de establecer una comunicación más directa entre candidatos y electores es uno de los puntos fuertes de los cambios que en este ámbito suponen las redes sociales. No obstante, más allá de la posibilidad de aumentar los espacios para la conformación de una discusión pública en el desarrollo de las campañas electorales, resulta preocupante que el tratamiento de los datos masivos aplicado en la contienda política pueda tener como consecuencia la creación de bases de datos conformadas de acuerdo con parámetros ideológicos[22].

4. La privacidad como mercancía: el negocio de los datos personales

En la actualidad se está produciendo una expropiación de la privacidad sin precedentes. Los datos personales se han convertido en un activo patrimonial de gran valor económico en el Mercado, el petróleo del siglo presente, ellos orientan el desarrollo y uso de nuevos productos y servicios[23]. 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, lo que da rienda suelta al mercadeo de datos personales sin demasiados problemas.

Estos dos factores han convertido a la privacidad en el producto estrella a comercializar por las grandes corporaciones del *Big data*. El negocio resulta más que rentable: los usuarios ceden gratuitamente sus datos personales (a cambio de la instalación de una App, mediante la suscripción a un boletín de ofertas

[21] Cfr. SOLOVE. "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, 2007, p. 757.

[22] Como apunta GARCÍA MAHAMUT, "Si no fortalecemos los aspectos legales referidos a que los partidos puedan a través de la tecnología realizar acopio masivo de datos personales de electores y potenciales votantes, lo que les permitirá sin demasiados problemas realizar una mega base de datos de perfil ideológico, nos encontraremos ante muy serios y graves problemas. El tratamiento de la información personal por nuevas tecnologías que hacen un uso masivo y profundo de los datos personales alcanzará un impacto en la esfera privada sin parangón. Si la información personal a cada minuto que pasa alcanza un mayor valor económico, el de las preferencias políticas resultará incalculable". Cfr. "Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español", *UNED. Teoría y Realidad Constitucional*, nº 35, 2015, p. 334.

[23] De acuerdo con MORENO MUÑOZ: "los datos son hoy el propulsor de crecimiento y transformación, como lo fue el petróleo en su momento. Y los flujos de datos configuran hoy nuevas infraestructuras, nuevos modelos de negocio y nuevas economías, con nuevos actores en posición de monopolio y políticas estatales diferenciadas según las ventajas de partida para beneficiarse de las reglas de mercado". Cfr. "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", ob. cit., p. 9.

de un grupo empresarial, permitiendo la geolocalización del Smartphone, revelando todo tipo de información personal en una red social…) a empresas que se dedican a almacenarlos, venderlos a terceros o procesarlos para un tratamiento posterior, generalmente con objetivos de marketing.

No puede ignorarse que el uso o la instalación de la mayoría de servicios y aplicaciones informáticas aparentemente gratuitas suponen auténticos contratos de adhesión (sobre los cuales sus consumidores no tienen capacidad alguna de negociación) que contienen, en su mayoría, un alto número de cláusulas abusivas, dónde los usuarios ceden sus datos personales –en ocasiones sin autorización expresa o incluso sin su conocimiento[24]– en contraprestación por los servicios recibidos, que más tarde se monetizan por dichas empresas dedicadas, en el fondo, al almacenaje, tratamiento, explotación y venta de datos personales.

También queda patente como las corporaciones de Internet y los operadores de telecomunicaciones han adquirido sobre los usuarios una capacidad de condicionamiento (e, indirectamente, control) sin precedentes. Acceden y patrimonializan nuestra privacidad por medio de la entrega de servicios aparentemente gratuitos que conllevan unilateralmente cláusulas abusivas respecto de los datos personales de los 'beneficiarios', sometidos desde ese momento a una constante vigilancia.

Así, los usuarios de estos servicios ya no somos meros consumidores pasivos sino que, a través de una pérdida considerable de nuestra privacidad, nos hemos convertido en parte del producto cuya ganancia, sin embargo, no percibimos. Sin ser del todo conscientes hemos evolucionado del Internet de las cosas[25] al Internet de las corporaciones, donde las cosas somos nosotros y en el que los datos personales son el nuevo producto a comercializar[26].

[24] 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.

[25] Término acuñado por ASHTON. "That 'Internet of Things' Thing", *RFID Journal*, 2009. Se aplica esta denominación a un sistema ciberfísico donde los objetos pueden conectarse a Internet a través de sensores ubicuos, dotándoles de funcionalidades decisivas en términos de disponibilidad, acceso, eficiencia en la distribución y contextualización. Se origina ligado al estándar de identificación automática para sensores de identificación por radio-frecuencia. Este sistema permite el almacenamiento y recuperación de datos remotos a través de dispositivos denominados etiquetas (pegatinas, tarjetas, transponedores…). Cfr. MORENO MUÑOZ. "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", ob. cit., p. 7.

[26] Cfr. DEL FRESNO GARCÍA. "Internet como macromedio: la cohabitación entre los medios sociales y los medios profesionales", *Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*, nº 99, 2014, pp. 107-110.

Si bien es cierto que, al menos en territorio europeo, están explícitamente reconocidos una serie de derechos en torno a la privacidad, en la práctica se ha producido un éxodo masivo de las principales empresas de Internet hacia territorio estadounidense, mucho menos garantista en la materia, tratando de extender el modelo norteamericano más allá de sus fronteras.

En la práctica, aprovechándose de la tentación o dependencia digital de las personas, empresas como *Google* o *Facebook* están llevando a cabo un tratamiento masivo de datos personales. Los usuarios firman un cheque en blanco sobre sus datos al aceptar los términos y condiciones de uso que éstas imponen siendo que, una vez dado su consentimiento a la política de privacidad que se ofrece en un paquete compacto e indesligable, resulta verdaderamente difícil seguirles la pista[27]. Esta situación escapa al control del usuario y es más que evidente la inseguridad jurídica que le acarrea como ciudadano, sujeto de irrenunciables derechos fundamentales. ¿Cómo puede solicitar la cancelación de una información sensible, puede que la más privada, si no tiene a quién dirigirse ni siquiera conoce a ciencia cierta qué saben de su vida? Pese a tener reconocidos explícitamente en nuestro ordenamiento derechos fundamentales como la intimidad o la protección de datos, éstos se convierten *de facto* en papel mojado.

Parece ser que tanto usuarios -obligados a pleitear en jurisdicción estadounidense- como gobiernos -que ven como las grandes corporaciones esquivan el cumplimiento de su ordenamiento jurídico- están tomando consciencia de los peligros de comercializar con la información más personal, escenario que ha dado lugar a la creación de un nuevo Reglamento Europeo de Protección de Datos.

5. Reflexiones finales

Como ya se ha observado, los datos no son neutrales en la medida en que están sujetos a todo tipo de condicionamientos, desde el diseño tecnológico hasta el soporte digital en el que son utilizados, así como las finalidades para las cuales se emplean. Ello produce sin ningún lugar a dudas, problemas de discriminación de diversa índole, en tanto que su parcialidad, consciente o inconscientemente, parece ser inevitable.

[27] Sobre esta cuestión, ALBERTO GONZÁLEZ plantea sus dudas sobre la legitimidad de la reutilización de los datos previamente cedidos para la realización de una compra o transacción, en tanto que la finalidad de elaborar perfiles de consumo para luego ser ofertados a terceros resulta ajena a la relación contractual inicial. En este sentido, considera que "esto constituye una desviación de la finalidad, para cual se necesitaría una nueva legitimación en base al consentimiento". Cfr. "Responsabilidad proactiva en el tratamiento de datos masivos", *Dilemata*, nº 24, 2017, p. 121.

El empleo indiscriminado del *Big data* tiene consecuencias sociales, políticas y económicas reales, hoy en día puestas de relieve, por el uso de *bots* y por las *Fake news*, abonando un campo de cultivo para la posverdad sin precedentes[28]. Los prejuicios, ideologías, sesgos e intencionalidades actúan libremente en el *Big data*, sin ningún tipo de sometimiento al control democrático[29].

Así las cosas, el propio cambio de paradigma que representa este nuevo escenario exige reconstruir el ámbito de libertad personal de los sujetos así como su esfera privada, para que el proceder de las empresas tecnológicas, las corporaciones del *Big data* y los nuevos medios de información no supongan una minusvaloración de dichas nociones, tan estrechamente ligadas a la protección del libre desarrollo de la personalidad de la ciudadanía. Efectivamente, un cambio de tal magnitud como el *Big data*, que sin duda representa un avance notable para el progreso social, debe cohonestarse con una respuesta efectiva desde el ordenamiento jurídico, para así adecuar sus proposiciones a los presupuestos estructurales de la protección de la privacidad. En otras palabras, es necesario realizar un esfuerzo desde el ámbito de las ciencias jurídicas para así elaborar propuestas doctrinales que, siendo compatibles con los beneficios propios de la revolución tecnológica, no permitan un retroceso en la protección de los derechos y libertades de la ciudadanía.

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 íntimos del individuo.

Teniendo en cuenta las circunstancias anteriormente mencionadas y con la pretensión de dotar de una mayor seguridad jurídica a los ciudadanos, el 4 de mayo de 2016 se publicó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las

[28] Como ejemplo, el *chatbot* Tay (sistema virtual de imitación del comportamiento humano capaz de generar conversaciones que simulan el lenguaje de las personas) diseñado por Microsoft para contestar las preguntas que los internautas quisieran hacerle así como entablar conversaciones, que tuvo que ser retirado en menos de 24h desde su puesta en funcionamiento al convertirse en un robot machista, homófobo y racista que, entre otras cosas, negaba el genocidio nazi o apoyaba la construcción de un muro entre EEUU y México.

[29] Ello puede observarse en el sesgo ideológico de los buscadores web, que posicionan los resultados en función de sus propios criterios –éstos, además, están abiertos a acuerdos comerciales pues ciertamente existe un mercado donde comprar un mejor posicionamiento web– o de las redes sociales que, mediante el uso de algoritmos, proporcionan a sus usuarios informaciones afines a su ideología así como les sugieren contenido contrastadamente vinculado a sus intereses, limitando con ello la capacidad crítica de los usuarios.

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)[30].

La nueva normativa asume como regla básica el hecho de que nuestra información personal debe estar sometida a nuestro propio criterio, pretendiendo 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[31].

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.

Entre los derechos de nueva incorporación destaca preeminentemente el derecho de supresión, popularmente conocido como el derecho al olvido, permitiendo a todo interesado obtener el borrado de sus datos personales cuando concurran ciertas circunstancias, tratando de proteger la privacidad de las personas frente a los retos que han propiciado la aparición de las nuevas tecnologías en connivencia con Internet.

En la actualidad, viviendo en plena sociedad de la información y del conocimiento, dónde la era digital es una realidad asumida plenamente y en la cual se avecinan nuevos retos inmediatos debido, principalmente, a la proliferación de la inteligencia artificial, el derecho al olvido se presenta como una suerte de garantía personal que aspira a poner remedio a los inconvenientes y perjuicios que genera la enorme multiplicación de datos personales que pasan a engordar bancos de almacenamiento y procesamiento fuera de nuestro control.

Junto al derecho al olvido, se ha procedido a la incorporación inmediata al ordenamiento jurídico español de toda una serie de nuevos "derechos digitales" mediante la nueva Ley Orgánica de

[30] 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.

[31] No obstante 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.

Protección de Datos Personales y Garantía de los Derechos Digitales, en algunos aspectos tan polémica. Entre éstos, merece destacarse el derecho a la neutralidad de Internet, a la educación digital, a la desconexión digital en el ámbito laboral o al acceso universal a Internet.

Se desarrollan así un conjunto de nuevos derechos fundamentales, como respuesta jurídica de la exigencia que la nueva realidad social venía reivindicando para el Estado social y democrático de Derecho, en tanto que éste debe adecuar sus presupuestos estructurales al cambio de paradigma que representa el *Big data*. El desarrollo de nuevos derechos, supone una necesidad imperante en el avance de la ciencia jurídica, en tanto que ésta requiere de una adaptación al contexto expuesto, para así garantizar la seguridad jurídica y la protección de los derechos y libertades de la ciudadanía.

Sin embargo, más allá de la voluntad garantista de las nuevas legislaciones en materia de protección de datos, no puede ocultarse otro propósito, quizás aún mayor, esto 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[32]. Por otra parte, para una verdadera garantía de los derechos fundamentales en este ámbito se necesita necesariamente contar con la complicidad y el compromiso de aquellos que diseñan dichos productos y servicios 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. Sólo una actuación conjunta y transversal puede arrojar luz a la cuestión, esperemos que así sea.

[32] Hecho que se ejemplifica mediante lo ocurrido con el *Safe Harbor* y la Sentencia del TJUE de 2015 en el *caso Schrems (*STJUE de 16 de octubre de 2015, asunto C-362/14*)* que lo declaró inválido y como, en la actualidad, mediante el acuerdo *Privacy Shield* se sigue permitiendo, de facto, especular con los datos personales de los ciudadanos, haciendo de las transferencias internacionales de datos la regla general y no la excepción.

6. Referencias bibliográficas

ALBERTO GONZÁLEZ, P . "Responsabilidad proactiva en el tratamiento de datos masivos", *Dilemata*, nº 24, 2017.

ASHTON, K. "That 'Internet of Things' Thing", *RFID Journal*, 2009.

BAUMAN, Z . *Modernidad líquida*, Fondo de Cultura Económica, Madrid, 2017.

BENTHAM, J. *Panóptico,* Círculo de Bellas Artes, Madrid, 2011.

CLARKE, R. *Introduction to Dataveillance and Information Privacy*, Australian National University, 2006.

DEL FRESNO GARCÍA, M. "Internet como macromedio: la cohabitación entre los medios sociales y los medios profesionales", *Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*, nº 99, 2014.

DÍEZ-PICAZO, L. *Experiencias jurídicas y teoría del Derecho*, Ariel, Barcelona, 1983.

FOUCAULT, M. *Vigilar y castigar. Nacimiento de la prisión*, Siglo XXI, Madrid, 2009.

GARCÍA MAHAMUT, R. "Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español", *UNED. Teoría y Realidad Constitucional*, nº 35, 2015.

HAN, B.C. *Psicopolítica*, Herder, Barcelona, 2014.

HAN, B. C. *La sociedad de la transparencia*, Herder, Barcelona, 2013.

HARCOURT, B. *Exposed. Desire and Disobedience in the Digital Age*, Harvard University Press, Cambridge, 2015.

HARCOURT, B. "Governing, Exchanging, Securing: Big Data and the production of a digital knowledge", *Public Law and Legal Theory Working Paper Group*, Columbia Law School, 2014.

LERMAN, J. "Big data and its exclusions", *Stanford Law Review*, 66, 2013.

MAYER-SCHÖNBERGER, V./CUKIER, K. *Big data. La revolución de los datos masivos*, Turner, Madrid, 2015.

MONASTERIO ASTOBIZA, A. "Ética algorítmica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", *Dilemata*, nº 24, 2017.

MORENO MUÑOZ, M. Privacidad y procesado automático de datos personales mediante aplicaciones y bots", *Dilemata,* nº 24, 2017.

O'NEIL, C. *Armas de destrucción masiva. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, Madrid, 2018.

PÉREZ LUÑO, A. E. /GONZÁLEZ-TABLAS Y SASTRE, R. "Ciberciudadanía y teledemocracia", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro II, Dykinson, Madrid, 2013.

PUYOL MORENO, J. "Una aproximación a Big Data", *Revista de Derecho, UNED*, nº 14, 2004.

SOLOVE, D. "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, 2007.

SOLOVE, D. "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol. 154, nº 13, 2006.