BIG DATA O EL ARTE DE ANALIZAR DATOS MASIVOS. UNA REFLEXIÓN CRÍTICA DESDE LOS DERECHOS FUNDAMENTALES

BIG DATA OR THE SKILL OF ANALYZING MASSIVE DATA. A CRITICAL REFLECTION BASED ON HUMAN RIGHTS

VANESA MORENTE PARRA
Universidad Pontificia Comillas - ICADE

Fecha de recepción: 14-1-18
Fecha de aceptación: 5-9-18

Resumen: *"Big Data" es conocido comúnmente como la tecnología disruptiva de las cinco "v": volumen, variedad, velocidad, valor y veracidad, que se vale de un nuevo tipo de análisis de datos, consistente en la identificación de patrones conductuales y que, como consecuencia de ello, delimita un nuevo conocimiento sobre el individuo. Si bien Big Data supone una herramienta informática muy útil para sectores tales como el mercadotécnico, el sanitario, ambiental y el científico, entre otros, es innegable la situación de riesgo en la que se sitúan algunos bienes jurídicos como la información personal o el libre desarrollo de la personalidad a través del uso de Big Data. Los perfiles conductuales son utilizados como herramientas de selección y exclusión tanto de individuos como de grupos humanos, lo que puede llevar a la toma de decisiones basadas únicamente en criterios algorítmicos y con graves consecuencias para las personas. Esta posibilidad de "clasificación personal" puede poner en serio riesgo el valor más esencial de nuestro sistema jurídico-político, la dignidad humana.*

Abstract: *Big Data is commonly known as the disruptive technology of the five "v": volume, variety, speed, value and veracity, which uses a new type of data analysis, consisting of the identification of behavioral patterns and, as a consequence of it, it delimits a new knowledge about the individual. Although Big Data is a very useful computer tool for sectors such as the marketing, sanitary, environmental and scientific, among others, it is undeniable the risk situation in which some legal assets such as personal information or free development are located of personality through the use of Big Data. Behavioral profiles are used as selection and exclusion tools for both individuals and*

human groups, which can lead to decisions based solely on algorithmic criteria and with serious consequences for people. This possibility of "personal classification" can seriously jeopardize the most essential value of our legal-political system, human dignity.

Palabras clave: Big Data, protección de datos, perfil conductual, dignidad humana y Reglamento General de Protección de Datos
Keywords: Big Data, data protection, profiling, human dignity and General Data Protection Regulation

1. APROXIMACIÓN CONCEPTUAL A LA TÉCNICA DEL BIG DATA: ¿EN QUÉ CONSISTE LA NUEVA ALQUIMIA?

Cuando se aborda un tema de actualidad como es el del Big Data o tratamiento de datos masivos, se puede caer en la tentación de asumir el discurso distópico que normalmente se genera en torno a los avances científicos y tecnológicos. Por ello, es recurrente comparar el Big Data con el "Big Brother" creado por George Orwell en su novela "1984". No obstante, esta identificación se quedaría corta, ya que el Big Data no es solo un "panóptico digital"[1] que ve la realidad presente, sino que además es capaz de augurar un comportamiento futuro, es decir es una especie de oráculo digital.

El uso de la herramienta técnica del Big Data proporciona una mirada más profunda, una mirada de calado, que va más allá de lo evidente, como sucede en los cuadros de Guiseppe Arcimboldo[2], donde aparece un rostro o un perfil humano si observamos el bodegón en su conjunto y no como un mero conglomerado de frutas y hortalizas individuales y diferenciadas.[3] La finalidad primera del Big Data supone por tanto una mirada que no solo ve

[1] Byung-Chul Han afirma que el panóptico digital es más eficaz que el panóptico de Bentham ya que el primero funciona sin ninguna óptica perspectivista. La vigilancia no perspectivista es más eficaz porque puede producirse desde todas las partes e incluso desde cada una de ellas. Eso provoca que mientras los moradores del panóptico de Bentham son conscientes de la presencia constante del vigilante, los que habitan en el panóptico digital se creen en libertad. BYUNG-CHUL HAN, *La sociedad de la transparencia*, Herder, Barcelona, 2013, pp. 88 y 89. En el mismo sentido se posiciona Zygmunt Bauman al afirmar que el mundo actual es un "post-panóptico" ya que el observador digital puede es ubicuo, "puede instalarse en reinos inalcanzables", e incluso desaparecer. Z. BAUMAN y D. LION, *Vigilancia líquida*, Paidós, Barcelona, 2013, p. 5.

[2] Guisseppe Arcimboldo (Milán 1527-1593).

[3] También en otras disciplinas artísticas, como en el cine, podemos encontrar buenos ejemplos de esta mirada profunda que busca otras realidades. Por ejemplo, en la película de

sino que descubre, se trata de una mirada transformadora que obtiene un valor donde solo hay información en bruto, sin pulir. Del mismo modo que el alquimista con sus aleaciones pretende obtener oro, la técnica del Big Data a través de combinaciones de datos masivos obtiene un nuevo tipo de oro.[4]

Estamos en realidad ante una nueva tecnología de tratamiento y análisis de datos, o ante un nuevo método de trabajo en el procesamiento de información que puede incluirse dentro de las denominadas tecnologías disruptivas[5], entre las que se encuentran el *cloud computing*, el *data mining*, los *weareables*[6], etc. Si internet, soporte digital del que se vale la nueva técnica del Big Data, ha revolucionado completamente la manera en la que se comunica la humanidad, "el Big Data ha supuesto una nueva manera de procesar la información a nivel global".[7] Es un hecho constatable que el uso de nuevas herramientas tecnológicas como el Big Data nos ha situado en un nuevo paradigma epistemológico en el que ha cambiado irreversiblemente nuestra

Matrix de los hermanos Wachowski (1999), solo unos pocos elegidos son capaces de ver la realidad más allá de la lluvia binaria de la que está configurada la realidad.

[4] Viktor Mayer-Schönberger y Kenneth Cukier advierten que la revolución de Big Data consiste precisamente en dejar de ver la información como algo estático y con fecha de caducidad. Big Data convierte los datos en "la materia prima del negocio, en un factor vital, capaz de crear una nueva forma de valor económico". Además, Big Data solo tiene sentido en escalas grandes, de las que extrae nuevas percepciones o crea nuevas formas de valor, lo que ha venido a transformar significativamente no solo los mercados, sino al propio individuo e incluso a los gobiernos. V. MAYER-SCHÖNBERGER & K CUKIER, *Big Data. La revolución de los datos masivos*, Turner, Madrid, 2013, pp. 16 y 17.

[5] Las tecnologías disruptivas a su vez estarían enmarcadas en la categoría general de "tecnologías emergentes" que incluso se han llegado a denominar "convergentes". Las tecnologías convergentes son identificadas por las iniciales NBIC (nano, bio, info y cogno) haciendo referencia a la combinación de nanotecnología, biomedicina, informática y neurociencia. M. BONAZZI, "Reconstructing man? The power of converging technologies", 2006, *http://cordis.europa.eu/news/rcn/111117_es.html* (consultado en julio de 2018).

[6] El "cloud computing" es un espacio virtual del que cualquier usuario de internet puede disponer para almacenar y compartir grandes cantidades de datos; el "data mining" o "minería de datos" supone la búsqueda de información secundaria a través de análisis extractivos en grandes silos de datos; por último, los "wearables" o "dispositivos vestibles" son prendas de vestir que a través de microprocesadores pueden medir nuestra presión arterial, el ritmo cardíaco, la glucemia a través de la sudoración, etc. Estas prendas constituyen una herramienta muy prometedora sobre todo en el sector sanitario y en el mundo deportivo.

[7] N. MILÓN BELTRÁN, "Retos para la privacidad en la Era Digital. Análisis económico y filosófico político del capitalismo contemporáneo", *Sociología y Tecnociencia. Revista digital de sociología del sistema tecnocientífico*, vol. 2, núm. 5, 2015, p. 33.

manera de analizar y gestionar la medicina, las finanzas, el clima, etc.[8] El Big Data, apoyado sobre la Inteligencia Artificial, consigue no solo almacenar, combinar y analizar información ingente, sino que además puede hacer que las máquinas aprendan a resolver problemas tomando decisiones autónomas sin la intervención de un ser humano.[9] En resumen, Big Data es una *nueva tecnología* que se vale de un *nuevo tipo de análisis* de datos, consistente en la identificación de patrones conductuales y que, como consecuencia de ello, delimita una *nueva mitología*, pues genera la creencia de que Big Data proporciona un conocimiento o "inteligencia superior" basada en percepciones previamente imposibles.[10]

Sin embargo, lo que hemos hecho hasta ahora ha sido describir la técnica de Big Data desde una óptica objetiva. Si nos centramos en los sujetos intervinientes en los procesos descritos del Big Data encontramos tres tipos de sujetos: el sujeto que cede los datos, consciente o inconscientemente, y que podríamos denominar "sujeto cedente"; el sujeto que se vale de esta nueva técnica de análisis de datos masivos –por ejemplo las diferentes empresas que hacen uso de ello–, y que podemos denominar "sujeto usuario o consumidor"; y, por último, el sujeto que desarrolla los programas informáticos que procesan los datos masivos, es decir, los "analistas de los datos". Esto en lo que a los sujetos intervinientes corresponde, sin embargo habría que hacer alusión a una cuarta categoría de sujetos que son precisamente los "no intervinientes" en el desarrollo de las nuevas tecnologías en general, y del Big Data en particular. Situar el foco crítico sobre los "excluidos" del Big Data, supone asumir que esta nueva técnica disruptiva no solo constituye una posible amenaza para la privacidad, e incluso para el libre desarrollo

[8] S. BAROCAS & H. NISSENBAUM, "Big Data´s End Run around Anonymity and Consent", *Privacy, Big Data and the Public Good*, Cambridge University Press (Cambridge Books Online: *http://ebooks.cambride.org;* p. 46.

[9] L. COTINO HUESO, "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata*, num. 24, 2017, p. 132.

[10] D. BOYD & K. CRAWFORD, "Critical questions for Big Data. Provocations for a cultural, technological and scholarly phenomenon", *Journal Information, Communication and Society*, núm. 5, vol. 15, 2012, pp. 662 y 663. (consultado online *http://dx.doi.org/10.1080/1369118X.2012.678878* junio 2018). La relación del Big Data con una "inteligencia superior" recuerda al argumento de la película Minority Report (Steven Spielberg, 2002), donde tres personajes llamados "precognoscentes" son capaces de visualizar ciertos acontecimientos delictivos antes de que ocurran gracias a su capacidad de predecir el futuro inmediato. Valiéndose de estas "previsiones", la policía procedía a la detención de los "delincuentes potenciales" justo antes de que perpetraran el delito.

de la personalidad, sino que puede afectar significativamente al principio de igualdad propio de las sociedades democráticas.[11] Big Data puede operar omitiendo sistemáticamente a personas que viven en los "márgenes tecnológicos", ya sea a causa de la pobreza, su situación geográfica, su estilo de vida, o por cualquier otra causa que los saque del "data field". Esto puede tener una primera consecuencia más o menos irrelevante en términos sociales, como son los "errores de cálculo" que más adelante abordaremos y que, en principio, solo afectarían al cálculo estratégico formulado por los que hemos denominado "sujetos usuarios o consumidores" de la técnica del Big Data. Sin embargo, un análisis de datos masivos sesgado por la exclusión no aleatoria de determinadas masas sociales, puede tener una consecuencia de mayor calado ético y jurídico, ya que supone una infrarrepresentación de los "colectivos situados en la periferia del Big Data", arrojando una imagen distorsionada de la realidad social actual.[12] Por supuesto, esta es la consecuencia objetiva de aplicar un Big Data sesgado, aunque, como indica Jonas Lerman, también se derivan consecuencias subjetivas, ya que la "marginación" de ciertos colectivos sociales puede tener consecuencias preocupantes para su efectiva participación democrática, por ejemplo al omitir su voz en el espacio público digital.[13]

Más adelante veremos cómo cada uno de estos sujetos juegan un rol diferente en el proceso del tratamiento de datos masivos: los tres primeros tipos de sujetos –cedentes, usuarios y analistas–, van a tener diferentes grados de responsabilidad ética y jurídica en el escenario digital, mientras que el último tipo de sujeto, los "excluidos", van a erigirse como "acreedores" de una cuota participativa en el "ágora virtual" proporcionado por las nuevas tecnologías.

2. EL TRATAMIENTO DE LOS DATOS MASIVOS A TRAVÉS DE BIG DATA: ¿DE QUÉ NATURALEZA SON LOS RIESGOS DERIVADOS DEL BIG DATA?

Si bien es cierto que en el sector económico y comercial es costumbre analizar el mercado con la finalidad de obtener "patrones conductuales" o "perfiles

[11] J. LERMAN, "Big Data and its exclusions", *Stanford Law Review online*, vol. 66, núm. 55, 2013, pp. 56 y 57.

[12] Idem, p. 57.

[13] Idem, p. 59.

de consumo", no es menos cierto que con la llegada de Big Data la obtención de dicha codiciada información se ha hecho más factible y mucho más certera. Tanto el sector de la mercadotecnia, como el sector bancario, el de los seguros privados, e incluso el sector sanitario, ya se están beneficiando de las ventajas que ofrece el uso del Big Data, sobre todo por lo que supone de reciclaje de datos, de datificación de datos incuantificables, de impulso a la innovación y al desarrollo, y por último, de ahorro significativo en algunos sectores tales como el sanitario.[14]

No obstante, un análisis meramente económico del Big Data sería realmente ciclópeo. Un fenómeno revolucionario como el de las técnicas disruptivas en general, y el del Big Data en particular, no puede ser analizado únicamente desde la perspectiva económica, e incluso desde la perspectiva técnica, sino que ha de ser analizado, especialmente, desde la óptica ético-jurídica.[15]

2.1. El criterio sociológico: las tecnologías disruptivas desde el prisma de los "riesgos civilizatorios"

Son muchas las voces que nos han advertido ya de los riesgos que se derivan de la sociedad de la información y la comunicación[16], y que se pueden

[14] Como señalan Omer Tene y Jules Polonestky, las empresas que usan Big Data para tomar decisiones empresariales se diferencian significativamente del resto. Según un informe del *McKinsey Global Institute* (MGI) ha quedado demostrado el efecto transformador que el Big Data ha tenido en sectores enteros que van de lo privado a lo público. El Big Data ayuda a las empresas a aumentar su productividad, los grandes datos permiten a los Gobiernos mejorar la administración del sector público y ayuda a las organizaciones globales a analizar la información para diseñar la planificación estratégica. Un ejemplo de ello es el conocido "Caso Vioxx´s". Vioxx era el nombre de un fármaco que fue retirado del mercado después de haberse podido comprobar, a través del análisis masivo de datos, que provocó más de 27.000 infartos de miocardio. También las empresas que suministran electricidad se valen del análisis de datos masivos para trazar un patrón de consumo energético. Otro sector económico que utiliza Big Data es el mercado minorista, donde se encuentran ejemplos como el de WalMart´s a cuyo uso debe en parte su éxito empresarial. O. TENE, J. POLONETSKY, "Big Data for All: Privacy and user control in the Age of Analytics", *Northwestern Journal of Technology and Intellectual Property*, vol. 11, núm. 5, 2013, pp. 244-246 y 249. (versión online consultada en julio de 2018).

[15] El Código de Buenas Prácticas en Protección de Datos para Proyectos Big Data clasifica los riesgos derivados de la aplicación del Big Data en dos bloques, siendo el primero el de los riesgos legales. Dentro de este bloque pone el acento en la falta de transparencia, en el problema de la manifestación del consentimiento informado, el establecimiento de "perfiles", la confusa procedencia de la información, el riesgo de la "reidentificación", y, por último, el plazo de conservación de los datos.

[16] B. C. HAN, *La sociedad de la transparencia*, Herder, Barcelona, 2016 o T. ROSZAK, *El culto a la información: un tratado sobre alta tecnología, inteligencia artificial y el verdadero arte de*

integrar en lo que Ulrich Beck denomina "riesgos civilizatorios".[17] El concepto de "riesgo civilizatorio" es acuñado por Beck para referirse a los alarmantes desafíos que acechan a las sociedades modernas, cuyo eje vertebrador es el capitalismo caracterizado por un insaciable y compulsivo consumo de recursos naturales, y que tiene como consecuencia inmediata la imparable emisión y vertido de sustancias tóxicas al medio ambiente.[18] Si bien, el autor mencionado pone su foco de atención en los riesgos ambientales y nucleares, podemos utilizar como analogía su modelo crítico para analizar los peligros derivados de la sociedad de la información y la comunicación, entendida también ésta como un sistema de consumo masivo de recursos, que en este caso es la información.[19] Los datos masivos se han convertido en la nueva materia prima –el nuevo petróleo– codiciada por los operadores económicos,[20] siendo una fuente inmaterial inagotable de generación de riqueza.[21] Por tanto: "en la modernidad avanzada, la producción social de riqueza va acompañada sistemáticamente por la producción social de riesgos".[22]

Los desafíos derivados de la sociedad tecnológica, o sociedad de la información y la comunicación, comparten ciertas características con los riesgos derivados de la sociedad industrial moderna. La primera característica compartida es que se trata de *riesgos futuros* o riesgos con potencialidad de mate-

pensar, Gedisa, Barcelona, 2009. Y en España véase M. CASTELLS, *La sociedad red: una visión global*, Alianza Editorial, Madrid, 2006.

17 U. BECK, *La sociedad del riesgo*… cit., p. 44.

18 Ulrich Beck, habla de un concepto de riesgo vinculado con dos fenómenos actuales, uno es la sobreproducción industrial actual, y otro es el desarrollo de la energía nuclear, sobre todo en su versión de bomba atómica. Es decir, se trata de riesgos propios de la "modernización", del "proceso civilizatorio de la modernidad". Por ello, el pensador alemán, parte de un concepto de riesgo universal, en relación con la comunidad global y no con los riesgos a los que se pueden ver expuestos individuos concretos en la sociedad tecnológica. U. BECK, *La sociedad del riesgo*, cit., p. 33.

19 Según Jeremy Rifkin en las últimas décadas las verdaderas revoluciones se producen cuando convergen dos factores: uno es el desarrollo de nuevas tecnologías de la comunicación y la información, y el otro es el desarrollo de nuevos sistemas energéticos. Es decir, que actualmente el desarrollo industrial y el avance de las TIC´s no pueden entenderse por separado. J. RIFKIN, *La tercera revolución industrial*, Paidós, Barcelona, 2011, pp. 14 y 15.

20 A. GARRIGA, "La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea", *Derechos y Libertades*, núm. 38, 2018, p. 111.

21 A. GARRIGA, *Nuevos retos a la protección de datos personales*, Dykinson, Madrid, 2016, p. 27.

22 Idem, p. 29.

rializarse a medio y largo plazo. Es decir, existen riesgos reales y presentes, cuya expresión menos lesiva podríamos encontrarla en el uso personalizado y sesgado de la información, ya sea ésta de carácter político o económico,[23] y cuya expresión más lesiva podría ser la directa violación del derecho a no ser juzgado por decisiones basadas en meros "perfiles" algorítmicos. Sin embargo, no podemos obviar el riesgo futuro e indeterminado que se cierne sobre el uso y abuso del análisis masivo de datos, sobre todo como potencial herramienta discriminadora. Y en atención a esta última idea, podríamos llegar a la conclusión de que como los riesgos que presenta la sociedad industrial –insaciablemente extractiva– son de naturaleza similar a los riesgos que se derivan de la sociedad de la información, pueden aplicarse los mismos remedios para intentar neutralizar dichos riesgos.

De lo que no cabe duda es que Big Data es la nueva alquimia, pues a través de la combinación o "aleación" de datos brutos y primarios obtiene valor agregado, es decir, puede obtener una información secundaria que no ha sido cedida voluntariamente y que tiene un valor incalculable. El rastro digital que dejamos los usuarios de internet a través de nuestras opiniones, consultas y búsquedas puede proporcionar un "conocimiento inferencial" que, en el peor de los casos, ayude a delimitar un "perfil sensible"[24]. Es decir, la combinación de datos masivos de carácter no sensible puede tener como

[23] La empresa Facebook ha estado envuelta recientemente en uno de los mayores escándalos de filtrado de datos masivos. Después de una investigación periodística llevada a cabo por varios medios de comunicación norteamericanos, salió a la luz a mediados del mes de marzo del presente año la filtración irregular de datos personales de cerca de 50 millones de clientes estadounidenses de la empresa Facebook a la compañía británica Cambridge Analytica. La consultora británica obtuvo los datos a través de una aplicación de perfilado psicológico desarrollada por un investigador de la universidad de Cambridge llamado Aleksander Kogan, que permitía acceder a información no solo de quienes utilizaban la herramienta, sino también de sus amigos. Supuestamente, los datos fueron recabados por Cambridge Analytica quebrantando las normas de Facebook. La información obtenida se utilizó para perfilar votantes y dirigirles propaganda política personalizada y noticias falsas. Eso les permitió influir en las elecciones estadounidenses de 2016 y también, a través de empresas vinculadas, en otros procesos electorales como el referéndum del Brexit. De este escándalo se derivaron dos consecuencias inmediatas para Facebook, la primera fue el denominado "carrusel de disculpas" que desde el mes de abril tuvo que emprender Mark Zuckerberg, como CEO de la empresa, comenzando en el Senado de los EE.UU y acabando en la sede del Parlamento Europeo en Bruselas. La segunda se ha manifestado en un cambio radical de las políticas de privacidad de la empresa, pasando a adoptar una filosofía de protección de datos proactiva tal y como le exige el nuevo Reglamento General de Protección de Datos en el espacio europeo.

[24] O. TENE, y J. POLONETSKY, "Big Data for All…", cit., p. 253.

resultado un conocimiento inductivo de carácter sensible, por ejemplo la orientación sexual, la ideología política, la confesión religiosa, etc. Big Data, a través de correlaciones masivas puede obtener información secundaria de carácter sensible, sobre la que se podrán adoptar futuras decisiones con efectos jurídicos o similares, y de las que se pueden derivar graves consecuencias para las personas.[25]

En segundo lugar, estamos ante *riesgos invisibles*. Si bien Beck se refiere al riesgo nuclear como el mayor riesgo invisible, también hace alusión al riesgo alimentario que se deriva del uso de pesticidas, a la contaminación del mar, al modo en que alimentamos a los animales, etc. En ambos casos se da la imposibilidad de "ponerse a cubierto", es imposible zafarse del riesgo.[26] Del mismo modo la sociedad 2.0 lo invade y gobierna todo –de ahí que la doctrina hable de la "dictadura de los datos"–, de tal manera que cada vez es más difícil abstraerse de esa realidad virtual de la que todos nosotros participamos voluntaria o involuntariamente. El panóptico digital ubicuo acecha constantemente sin ser visto y, lo que es peor, con nuestro beneplácito.[27]

En tercer lugar, se trata de *riesgos universales*, o como Beck los denomina "la globalización de los riesgos civilizatorios"[28]. El ciudadano actualmente es, voluntaria o involuntariamente, un "ciudadano digital". La participación en la ciudadanía digital puede ejercerse pasivamente: tanto la Administración Pública[29] como las empresas privadas exigen al individuo el procesamien-

[25] Sobre las "inferencias" en la era de los datos masivos véase S. BAROCAS, H. NISSENBAUM, "Big Data´s End Run around Anonymity and Consent", en *Privacy, Big Data and the Public Good*, Cambridge University Press, 2014, pp. 55 y 56.

[26] Algunos autores advierten de la imposibilidad de escapar de la era de los "datos masivos" como tampoco se puede escapar de la "globalización", de hecho puede afirmarse que el fenómeno del Big Data trae causa directa del proceso globalizador de las comunicaciones y la información. D. OPREA, "Big Questions on Big Data", *Revista de cercetare si interventie sociala*, vol. 55, 2016, p. 113 (*www.rsic.ro*) julio 2017.

[27] Ana Garriga, siguiendo la categorización de Zygmunt Bauman y de Byung-Chul Han vistas arriba, se refiere al "superpanóptico" como la vigilancia ubicua consentida por todos los usuarios de internet, que además se alimenta masivamente de ingentes cantidades de información disponible y en tiempo real. A. GARRIGA, "La elaboración de perfiles…", cit., p. 124.

[28] U. BECK, *La sociedad del riesgo*, cit., p. 52.

[29] Precisamente el origen del tratamiento y procesamiento automatizado de datos tiene su razón de ser en una demanda de la Administración Pública, concretamente para la elaboración del censo. En 1884 Herman Hollerith desarrolló un sistema de cómputo a través de tarjetas perforadas en la que los agujeros representaban el sexo, la edad o la raza. Este sistema de conteo poblacional redujo a la mitad del tiempo empleado por las diferentes administraciones públicas en esta empresa. V. MAYER-SHÖNBERGER, K. CUKIER, *Big Data. La revolución de*

to de sus datos en soporte digital, e incluso la solicitud de prestaciones y servicios públicos se hacen vía telemática[30]; o bien activamente dejando la "huella digital" en las redes sociales consultando blogs o páginas webs.[31] La vida digital visibiliza al ciudadano, incluso involuntariamente, como ponen de manifiesto Viktor Mayer-Schönberger y Kenneth Cukier cuando nos advierten de la posibilidad de establecer "perfiles en la sombra" a través de las interconexiones de los datos volcados por los titulares de cuentas en redes sociales.[32]

Si bien, para Ulrich Beck la contaminación y el riesgo nuclear tiene un efecto democratizador e igualador que convierte a la "sociedad del riesgo" en una sociedad sin clases, pues los riesgos tienen un "efecto boomerang", es decir se vuelven incluso contra el que, en un principio, se ha beneficiado de ellos,[33] no sucede lo propio con los riesgos derivados de la sociedad tecnológica. En internet hay diferentes categorías de "aparición" o "visibilización", una de ellas es el consumo, otra la participación en redes sociales –que incluso puede ser de naturaleza política o religiosa–, otra es la consulta a webs, blogs, etc., todas ellas trazan un rastro digital. A través de esta información,

---

los datos masivos, Turner, Barcelona, 2013, pp. 36 y 37 M. CASTELLS, *La era de la información: economía, sociedad y cultura*, vol. I (trad. Camen Martínez Gimeno y Jesús Alborés), 2ª edición, Alianza Editorial, Madrid, 1996, pp. 69 y ss. (versión on line: *http://www.felsemiotica.org/site/wp-content/uploads/2014/10/LA_SOCIEDAD_RED-Castells-copia.pdf*) octubre 2017.

30 Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

31 El 70% de la información digital es generada por nosotros mismos a través de nuestra interacción con los diferentes servicios en red, por lo que solo el 30% de nuestra información entra en internet de una manera "pasiva" podríamos decir. No obstante, ha de tenerse en cuenta la variabilidad potencial de esta última cifra a la luz del crecimiento constante del "internet de las cosas" –o internet 3.0–, esto es, todos aquellos aparatos electrónicos que se encuentra conectados a internet y que vuelcan en la red nuestra información de manera constante. Por ejemplo, todas las tecnologías vestibles se encuentran conectadas a internet y llevan un registro exacto de los indicadores que nos están midiendo, como pueden ser las pulsaciones, los niveles de glucemia en sangre o la presión arterial. A. GARRIGA, *Nuevos retos a la protección de datos personales*, cit., p. 29.

32 Los autores mencionados explican cómo a través de la interconexión de perfiles creados en internet se puede llegar a identificar a una persona relacionada con el "sujeto o sujetos fuente" sin que esta tenga creada una cuenta en la red social. Es decir, a través del cruce de información, se llega a la identificación de un tercero a través de un procedimiento inferencial, e incluso se puede llegar a conocer su orientación sexual. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data…*, cit., pp. 187 y ss.

33 U. BECK, *La sociedad del riesgo*, cit., p. 53.

o de su ausencia, las empresas e incluso las instituciones públicas pueden fijar perfiles o patrones conductuales, ideológicos, religiosos, etc., y, por consiguiente, se pueden llevar a cabo discriminaciones basadas en conclusiones algorítmicas. En el contexto de la sociedad de la información los datos gozan de la legitimidad que otorga el rigor científico –si es que entendemos que de la aplicación de técnicas como el Big Data se pueden obtener conclusiones "científicas"–, con la consecuencia de que los "perfiles conductuales", elaborados gracias a meros cálculos algorítmicos, van a gozar de una presunción de validez difícilmente cuestionable.

2.2. El criterio jurídico: ¿cuáles son los riesgos del Big Data para la dignidad humana?

Una vez analizados y categorizados los riesgos reales y potenciales que se pueden derivar de la aplicación de la técnica del Big Data, a través del marco crítico denominado "riesgos civilizatorios", y que agotan la crítica sociológica de esta nueva técnica disruptiva, podemos situarnos en el terreno del Derecho y analizar desde aquí el posible impacto de dicha técnica sobre los derechos fundamentales.[34] Si ponemos el foco de atención en el proceso técnico del Big Data comprobamos que en cada una de sus fases se pueden presentar riesgos de naturaleza ético-jurídica. En la primera fase del Big Data surge el *riesgo de la opacidad*,[35] ya que Big Data puede nutrirse de tan variadas fuentes que haga harto complicado saber cuál es el origen de la información recopilada, sobre todo porque la mayoría de los datos utilizados serán exógenos, es decir, el agente usuario de Big Data aportará bases de datos propias –datos endógenos– pero la mayoría de ellos serán recabados de bases de datos externas. El volumen y la variedad de las fuentes es tal que la propia

[34] Como afirma Ricard Martínez, "el proceso de transformación digital se produce en un contexto sociopolítico muy determinado, el del nacimiento en los últimos 250 años de los estados constitucionales, y el de la afirmación radical de la dignidad del ser humano y de los derechos fundamentales que la sustentan. De ahí, el impacto de la transformación digital no puede sino ser concebido desde la ética de los derechos humanos". R. MARTÍNEZ, "Cuestiones de ética jurídica al abordar proyectos de Big Data", *Dilemata*, num. 24, 2017, p. 154.

[35] No siempre el concepto de "opacidad" u "oscuridad" se ha relacionado de manera negativa con la técnica del Big Data. Woodrow Hartzog and Frederic Stutzman abogan por la "oscuridad desde el diseño" o la oscuridad en línea, a través de cuatro principios básicos: 1) Búsqueda visible, 2) Acceso desprotegido, 3) Identificación y, 4) Transparencia. W. HARTZOG, F. STUTZMAN, "Obscurity by Desing", *Washington Law Review*, núm. 88, 2013, pp. 388-389.

confusión[36] provoca la opacidad del proceso recopilador y su consecuente pérdida de control tanto por parte del propio titular de la información como del responsable del tratamiento,[37] sobre todo si el análisis de los datos masivos se externaliza en otra empresa o entidad a través de una subcontratación.

En la segunda fase del proceso de análisis de datos masivos, se produce el *riesgo de la inconmensurabilidad*, estrechamente relacionado con el anterior. Si se desconoce el origen de la información y, además, se desconoce el número exacto de datos procesados, ya que se trata de datos masivos, va a resultar bastante complicado otorgar una protección plena y efectiva a ciertos bienes jurídicos, como la intimidad y el libre desarrollo de la personalidad. No obstante, no se trata solo de un problema cuantitativo sino también cualitativo. Big Data opera tanto con datos personales como con datos anónimos, de hecho, las empresas y organismos públicos y privados que utilizan esta técnica, en realidad no buscan la identificación personal a través de datos concretos como puede ser el nombre, el domicilio, la edad, el sexo, etc., sino que lo que buscan es la identificación de "comportamientos concretos", que de manera indirecta sí pueden llevar a la identificación de los individuos. Si no es posible saber con exactitud cuántos son los datos utilizados por Big Data, ni tampoco es posible precisar de qué naturaleza son dichos datos, es decir si son personales, codificados o anónimos, el Derecho se encuentra ante un serio problema de "déficit de garantía jurídica", o ante un problema de "inseguridad jurídica", ya que no se puede proteger lo que no se conoce.

---

[36] Según Mayer-Schönberger y Cukier pretender entrar en el mundo de los datos masivos con el esquema mental de la era analógica, basada en la búsqueda permanente de la exactitud, supone cometer un error de bulto. Aunque en un primer momento pueda parecer contraintuitivo, afirman que tratar los datos como algo imperfecto e impreciso nos permite afinar en los pronósticos y así comprender mejor nuestro mundo. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data*…, cit., pp. 58 y 59. Tomás Aluja nos advierte de que mientras que la Inteligencia Artificial se preocupa más por ofrecer soluciones algorítmicas con un coste computacional aceptable, la estadística se ha preocupado más del poder de generalización de los resultados obtenidos, esto es, de poder imputar los resultados a situaciones más generales que la estudiada. Véase T. ALUJA, "La minería de datos, entre la estadística y la inteligencia artificial", *Qüestiió*, vol. 25, núm. 3, p. 481.

[37] Es lo que Ana Garriga denomina "los datos invisibles para los usuarios de internet". A. GARRIGA, "La elaboración de perfiles…", cit., p. 109. Neil Richards y Jonathan King entienden que la "transparencia" es una de las tres paradojas que se derivan de la aplicación del Big Data, ya que, según estos autores, el Big Data recaba la información personal para hacer que el mundo sea más transparente, pero en realidad el tratamiento que hace de los datos y las herramientas que utiliza para llevar a cabo dicho tratamiento es opaco. N. M. RICHARDS, J. H. KING, "Three paradoxes of Big Data", *Stanford Law Review Online*, núm. 66 vol. 41, 2013, p. 42.

Podría pensarse que una posible solución a este problema vendría dada por la exigencia de dar más y mejor información al afectado, no obstante, "más información no conduce de manera necesaria a mejores decisiones", sino que con frecuencia *menos* puede ser *más*.[38] Si el responsable del tratamiento de los datos debe informar absolutamente de todo a los afectados, éstos otorgarían su consentimiento por "agotamiento" en un contexto saturado de información.[39] En un escenario semejante, el derecho fundamental a la protección de datos personales puede ahogarse en un profundo océano de información masiva y caótica que haga impracticable la obtención de un consentimiento informado de pleno derecho como veremos en lo sucesivo.

En la tercera y última fase del Big Data encontramos los tres tipos de resultados o modelos analíticos que se pueden alcanzar con la aplicación de Big Data. El primer modelo es el *predictivo* con el que se evalúa la probabilidad que tiene un individuo concreto de mostrar un comportamiento específico en el futuro, esto, fija un perfil conductual individual y futuro.[40] El segundo modelo es el *descriptivo* con el que se clasifica a los individuos en grupos, esto es, busca la identificación de las relaciones intersubjetivas dentro de un mismo grupo o comunidad. El tercer y último modelo es el de *decisión*, con el que se describe la relación entre todos los elementos de una decisión, incluidos los resultados de los modelos de predicción, la decisión a tomar y el plan de variables y valores que determinan la propia decisión, con la finalidad de predecir los resultados mediante el análisis de muchas variables.[41]

Solo a través de la práctica de los dos primeros modelos, el predictivo y el descriptivo, podemos llegar al tercero, es decir, a la toma efectiva de una decisión basada en los parámetros informativos proporcionados por los dos primeros estadios. Si bien es cierto que el establecimiento de perfiles de consumo es una práctica que se ha venido utilizando cada vez más en los

[38] B. C. HAN, *La sociedad de la transparencia*, Herder, Barcelona, 2016, p. 17.

[39] El cansancio de la información, o por sus siglas en inglés IFS (Information Fatigue Syndrom), es la enfermedad psíquica que se produce por un exceso de información, según el psicólogo David Lewis que fue quien acuñó el término en 1996. Los afectados se quejan de crecientes parálisis de la capacidad analítica, perturbación de la atención, inquietud general o incapacidad de asumir responsabilidades. B. C. HAN, *En el enjambre*, Herder, Barcelona, 2018, p. 88.

[40] Gracias al Big Data se permite generar "patrones dinámicos de tendencias de futuro", a través de su potencial predictivo decisivo en muchos casos para la toma de decisiones. L. COTINO HUESO, "Big Data e Inteligencia Artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata*, núm. 24, 2017, pp. 133.

[41] Véase Informe sobre Big Data y salud digital elaborado por la Fundación Vodafone España y Red.es Ministerio de Energía, Turismo y Agenda Digital en 2017, pp. 19 y 20.

últimos años, no es menos cierto que la llegada de Big Data ha perfeccionado significativamente la técnica del "perfilado"[42], tanto individual como grupal. Es precisamente en la última fase del Big Data donde se obtiene, como resultado de la recopilación masiva de datos y de la combinación de los mismos, el establecimiento de "patrones de conducta" que no solo describen la realidad presente sino, y lo que es más importante, muestran un futuro probable.[43] Estos "patrones conductuales" o "perfiles comportamentales" se basan en correlaciones algorítmicas que, como advierte Elena Gil, pueden tener su razón de ser en relaciones entre variables de naturaleza espuria o falsa, favoreciendo correlaciones erróneas por azar o confusión.[44] Pero se pueden dar más errores, como el "error del sesgo de confirmación". Cuando las empresas fijan perfiles a través del uso del Big Data lo que buscan en realidad es confirmar un punto de vista o una opinión –incluso un prejuicio– preexisten mediante un uso selectivo de los datos. Es decir, se producen los denominados "falsos positivos".[45]

La posibilidad de que puedan darse en la realidad estos errores y sesgos justificaría la promoción de un riguroso juicio crítico tan intuitivo como científico sobre los resultados obtenidos a través del Big Data. Es decir, la más que posible materialización de estos riesgos potenciales exigiría una ineludible intervención humana cualificada y objetiva con la que evitar el *riesgo de deshumanización*,[46] que constituiría el tercer riesgo, en este caso de naturaleza más ética que jurídica en realidad. Sin embargo, el procedimiento automatizado de datos que busca la fijación de perfiles conductuales parece ir en sentido contrario, ya que supone la minimización o anulación intencionada de

[42] El 4.4 del 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 entiende por "perfil" lo siguiente: "*toda forma de tratamiento automatizado de datos personales consistente en evaluar determinados aspectos personales de una persona física, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, comportamiento, preferencias, salud, etc.*".

[43] Esto es lo que se ha denominado "analítica predictiva", como la "ciencia" que puede predecir el comportamiento de los individuos a través de la información que, directa o indirectamente, van volcando en internet. E. SIEGEL, *Analítica predictiva: predecir el futuro utilizando Big Data*, Anaya, Madrid, 2013.

[44] E. GIL, *Big Data, privacidad y protección de datos*, Agencia Española de Protección de Datos, Boletín Oficial del Estado, Madrid, 2016, pp. 32 y ss.

[45] Véase R. HERSCHEL & V. M. MIORI, "Ethics & Big Data", *Technology in Society*, núm. 49, 2017, p. 32, disponible en *www.elsevier.com/locate/techsoc* (consultado en julio 2017).

[46] E. GIL, *Big Data, privacidad y protección de datos*, cit., pp. 32-43.

la intervención humana en dos momentos concretos: *a priori* o momento en el que se analizan los datos masivos, lo que debe entenderse como "pérdida del valor de la intuición"; y *a posteriori* como "pérdida del juicio crítico", y de la empatía, entendida como aquella capacidad humana de "ponerse en el lugar del otro". Para algunos estudiosos del fenómeno Big Data, en el proceso del análisis de datos masivos el factor humano queda reducido al papel del "analista de los datos" o "científico de los datos". El científico de los datos no solo tiene como cometido el desarrollo del proceso de recolección, selección y combinación de los grupos de datos a través de la elaboración de los algoritmos adecuados, sino que debe interpretar la información resultante de dicho proceso. De ahí que, además de creadores y desarrolladores del proceso del Big Data, los "científicos de datos" son los intérpretes del Oráculo, que tendrán que traducir al lenguaje natural lo que solo a ellos les revela el lenguaje matemático de los algoritmos. Incluso, se ha desarrollado toda una "hermenéutica de la ciencia de los datos", la cual debe basarse en siete puntos: 1) interdisciplinariedad; 2) generación de significado; 3) habilidad práctica; 4) conocimiento del contexto histórico; 5) reconocimiento de los propios prejuicios; 6) importancia de la comunidad como entendimiento común; y 7) rechazo de un significado único y objetivo.[47]

Si bien estos siete criterios pueden ayudar a objetivar en alguna medida la decisión algorítmica, aquí se apela al "factor humano" como única garantía para cubrir aquellos ámbitos que nunca podrán ocupar las máquinas o los algoritmos. A pesar de que actualmente se ha demostrado que las máquinas pueden aprender a través de los procesos de "machine learning", y los algoritmos pueden mejorarse permanentemente mediante el "aprendizaje automático",[48] hay ámbitos que son –y quizá deban seguir siéndolo– esencialmente humanos y que como ya se ha indicado, podemos identificar con "el conocimiento intuitivo" y con la capacidad de "empatizar" con otros seres humanos.[49] Es cierto que tanto el "conocimiento intuitivo" como

[47] M. FULLER, "Big Data: New Science, New Challengers, New Dialogical Opportunities, *Journal of Religion & Science*, 2015, pp. 576-578

[48] B. D. MITTELSTADT, P. ALLO, T. MARIAROSARIA, S. WACHTER y L. FLORIDI, "The Ethics of algorithms. Mapping the debate", *Big Data & Society*, 2016, p. 3

[49] Facebook cuenta con un equipo humano de 20.000 "moderadores", de los cuales 7.500 son "revisores de contenido", cuya función consiste en revisar o evaluar los contenidos que diariamente vuelcan los usuarios de la red social. En realidad de trata de "censores de contenidos", ya que se dedican a analizar todas las imágenes y los textos que aparecen en la red social con la finalidad de eliminar aquello que entienden cultural o moralmente incorrecto

la "inteligencia intuitiva" han sido analizadas desde diferentes campos de conocimiento,[50] sin embargo en la actualidad son la psicológica cognitiva y la neurociencia las disciplinas que están dedicando más atención a su estudio. Desde estas disciplinas cada vez se está afirmando con más vehemencia que las decisiones basadas en la intuición no son irracionales y que aceptar cierto margen de incertidumbre puede ayudarnos a escoger el mejor camino. Nuestro cerebro inconsciente nos ayuda a decidir rápidamente ante situaciones confusas donde la información puede ser caótica. Es lo que comúnmente se ha denominado "corazonada".[51] La neurociencia nos dice que el cerebro inconsciente, entendido como herramienta básica para tomar decisiones en nuestra vida diaria, es imprescindible y por consiguiente insustituible. Las máquinas están programadas para tomar decisiones de un modo lógico-matemático, puramente racional, por lo que quizá la pérdida de la intuición como "factor humano" sea un lujo que no nos podamos permitir como especie.[52] Esto nos lleva a afirmar que la inteligencia artificial no es una inteligencia equiparable u homologable a la humana, ya que, como dice Ricard Martínez, es una inteligencia incapaz de percibir las sutilezas emocionales que intervienen en la adopción de cualquier tipo de decisión. Además, la neurociencia viene demostrando hasta qué punto emociones como la empatía o la solidaridad se encuentran en la base de decisiones irracionales, desde el punto de vista de una máquina, pero que resultan cruciales para nuestro éxito como especie.

Por ello, la necesaria presencia del "factor humano" en las decisiones automatizadas garantiza una cuota mínima de empatía,[53] a través del es-

---

o inapropiado, como por ejemplo escenas excesivamente violentas o pornográficas, que pueden acabar con la imagen "familiar" que pretende proyectar la empresa.

[50] El intuicionismo ha sido abordado desde diferentes disciplinas y por diferentes autores, por ejemplo en la psicología destacan Sigmund Freud y Howard Gardner; en la sociología Malcolm Gladwell; en la filosofía Edmund Husserl y Henry Bergson; desde la filosofía moral (intuicionismo ético) Michael Huemer; y por último, desde la filosofía política John Rawls.

[51] G. GIGERENZER, *Decisiones instintivas: la inteligencia del inconsciente*, Ariel, Barcelona, 2008, pp. 9 y ss.

[52] R. MARTÍNEZ, "Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos", *Dilemata*, num. 24, 2017, p. 154.

[53] La posibilidad de oponernos a las decisiones estrictamente automatizadas que nos afecten, es una buena muestra, afirma Federico de Montalvo, de cómo la intuición, el llamado ojo clínico, seguirá ostentando un papel protagonista en este nuevo mundo. La maquina ayuda pero nunca sustituye, mejora pero no completa el análisis y las conclusiones. F. DE MONTALVO, "¿Puede la máquina sustituir al hombre? Una reflexión jurídica sobre el ojo clínico y la responsabilidad en tiempos de Big Data", en Fronteras CTR, *Revista de Ciencia,*

tablecimiento de un espacio básico de fraternidad –que podemos denominar respeto a la dignidad humana–, con el que protegernos mutuamente de aquellas decisiones o medidas excesivamente "lógico-matemáticas" o "racionales" que nos puedan llevar a situaciones de injusticia e inequidad, intentando evitar con ello el clasificado como cuarto y último riesgo, el *riesgo de discriminación*.[54]

La realidad social actual se caracteriza básicamente por darse en un "escenario global" donde los actores principales no son los Estados soberanos, ni siquiera las agrupaciones políticas regionales constituidas por algunos de estos Estados, sino las grandes multinacionales como Facebook y Google, y que además son las encargadas de redactar el guión a seguir en el mercado de los datos que masiva y constantemente fluyen por internet.[55] Después del sonado escándalo de la empresa Cambridge Analytica citado anteriormente, podríamos pensar que los verdaderos administradores de una buena parte de la información personal que fluye por internet son las grandes multinacionales del sector digital y no los Estados soberanos.[56]

Posiblemente una de las razones por las que la UE aprobó en mayo de 2016 el nuevo Reglamento General sobre protección de datos personales fuera la necesidad de limitar, en cierto modo, el poder de las empresas que operan en internet, procurando así una mayor y mejor protección a nuestra privacidad. Como se verá en el epígrafe siguiente, la novedad significativa

---

Tecnología y Religión, septiembre de 2018, UPC-ICADE (revista online, consultada en octubre de 2018).

[54] Viktor Mayer-Schönberger y Kenneth Cukier abogan por la intervención en el proceso de análisis de datos y fijación de perfiles del "algoritmista externo", que vendría a ser una especie de auditor o evaluador externo no solo de los aspectos técnicos sino también de los aspectos éticos del proceso. El problema es que estos autores parecen reducir la función del evaluador externo a la de un mero "supervisor deontológico". Los mayores riesgos son para los derechos fundamentales y eso va mucho más allá de una supervisión de las reglas de conducta. V. MAYER-SCHÖNBERGER & K. CUKIER, *Big Data*…, cit., p. 222.

[55] Puede verse la generación de datos en internet en tiempo real en: *http://otae.com/internet-en-tiempo-real/#.W1XSDtUzbIU*

[56] La tercera paradoja que, según Richards Neil y Jonathan King, se deriva de la aplicación de Big Data es precisamente la del "poder". Big Data provoca un desequilibrio intolerable en una democracia, ya que son las grandes empresas informáticas las que disponen de la información suficiente como para orientar nuestra atención en función de sus necesidades. De ahí que estos dos autores apelen a la necesidad de establecer un equilibrio de poder entre quienes generan los datos y los que hacen inferencias y toman decisiones basadas en dichos datos. En caso contrario, nuestras democracias se pueden ver seriamente afectadas. N. M. RICHARDS & J. H. KING, "Three paradoxes of Big Data", cit., p. 45.

en la política de privacidad que nos trae el RGUE se da en el cambio de una filosofía reactiva a una filosofía de protección de datos proactiva, que además empodera al titular de los datos con la intención de que sea el propio sujeto el que gestione el flujo de su información personal en internet. Si bien este hecho podría hacernos recobrar cierta confianza en la necesaria diligencia empresarial en relación con la guarda y custodia efectiva de nuestra información personal, voces autorizadas en el sector nos advierten de que el problema es nuclear, en el sentido de que el modelo de negocio de las grandes compañías de internet está precisamente en el uso de los datos de los usuarios, los cuales se utilizan para desarrollar mensajes publicitarios personalizados y, por consiguiente, más efectivos. De tal manera que, como afirma Sandy Parakilas, exdirector de operaciones de red social en Facebook, "el uso de los datos para armar perfiles de usuarios y predecir comportamientos es algo que no tiene precio para las compañías". Este modelo de negocio exige que los servicios proporcionados por las redes sociales y las compañías *online* traten de convertir sus servicios en más y más adictivos, porque cada minuto que pasamos en uno de sus servicios se traduce en dinero para la empresa, el menos en términos de anuncios y publicidad.[57]

Sin embargo, parece claro que el "perfilado conductual" en el ámbito comercial no supone ningún problema ético-jurídico a priori, ya que no se afecta a ningún bien jurídico susceptible de protección. Sin embargo, sí podemos plantearnos la licitud de los perfilados políticos, jurídicos o sociales, a través de los cuales internet nos etiqueta, nos clasifica o nos adhiere a un grupo social, a una corriente de pensamiento determinada, a un partido político[58] o a una religión, sin que nosotros hayamos manifestado nuestro consentimiento. El problema se agrava si además tenemos en cuenta que este tipo de información es de carácter sensible, lo que nos puede convertir, sin ser nosotros conscientes de ello, en personas en situación de vulnerabilidad. La pregunta que debemos plantearnos seguidamente es si el nuevo RGPD de la UE viene a dar solución efectiva a este tipo de problemas que afectan directamente a algunos derechos fundamentales.

[57] Sandy Parakilas trabaja actualmente en *Center for Human Technology*, organización que aboga por mejorar la relación de las personas con los dispositivos y servicios como medios sociales.

[58] La obtención de "perfiles políticos" sin consentimiento expreso es uno de los problemas que plantea la nueva Ley española de Protección de Datos y derechos digitales LO 3/2018 de 5 de diciembre de 2018.

2.2.1 El Reglamento General de Protección de Datos de la UE: hacia una política proactiva en la protección de datos personales

Como se ha advertido arriba, determinados usos o aplicaciones de las denominadas tecnologías disruptivas pueden poner en riesgo algunos de los bienes jurídicos que en la actualidad occidental gozan de mayor predicamento, como son la privacidad y el libre desarrollo de la personalidad. En esta ocasión, la UE[59] ha tenido claro que otorgar una protección efectiva a estos derechos pasa, ineludiblemente, por la consolidación de una filosofía de protección de datos personales basada en dos pilares fundamentales: por un lado, una filosofía de la responsabilidad proactiva, dirigida a los responsables y encargados de los diferentes tratamientos de datos personales; y, por otro lado, una filosofía de empoderamiento, dirigida a los sujetos titulares de la información personal. El RGPD de la UE ha venido por tanto a implantar una nueva filosofía de protección de datos de naturaleza positiva, basada en la responsabilidad proactiva y preventiva –frente a los mecanismos de carácter reactivos que hasta la fecha habían regulado la materia–. Esta nueva política de protección de datos se estructura en torno a un grupo de principios fundamentales, a saber: el "principio de seguridad proactiva"[60]; el "principio de transparencia" que pretende garantizar un tratamiento de datos claro para el "sujeto cedente" de dichos datos, pero que a su vez sea un procedimiento opaco ante posibles intromisiones externas no justificadas o no autorizadas, lo que tendrá que hacerse a través del denominado "cifrado de datos" o "codificación segura" de los datos;[61] el "principio de minimización

[59] Véase el Programa Marco de la Unión Europea, que en esta ocasión se ha denominado Hirozonte2020 (H2020). Desde el año 2014 la UE ha implantado tres pilares de actuación, desde los que se pretende abordar los principales retos sociales, promover el liderazgo industrial en Europa y reforzar la excelencia de su base científica.

[60] que se da a través de dos vías: la seguridad desde el diseño y la seguridad por defecto, a lo que hay que añadir el procedimiento de evaluación sobre el impacto en la privacidad que puede provocar el filtrado de datos, los denominados PIA por sus siglas en inglés (Privacy Impact Assesment), dirigidos fundamentalmente al responsable y al encargado del tratamiento de los datos personales.

[61] Si bien, el cifrado y la encriptación de los datos personales es la piedra angular de un tratamiento seguro y confidencial, no es menos cierto que en un marco de análisis de datos masivos, existe un alto riesgo de conseguir la "reidentificación" de un individuo, incluso partiendo de datos anónimos. Para algunos autores, una buena manera de salvar este problema podría consisir en entender que todos los datos, personales, seudoanonimizados y anónimos, sean tratados como si de datos personales se tratase. Es decir, los datos personales deberían definirse por una "matriz de riesgo" teniendo en cuenta el riesgo, intención y posibles conse-

de los datos",[62] que consiste en usar única y exclusivamente los datos que son necesarios para alcanzar las metas o los objetivos, privados o públicos, previamente establecidos; el "principio de limitación del uso de los datos personales"; y por último el "principio de autonomía o autodeterminación del individuo sobre su propia información".

2.2.2. *Los perfiles conductuales como factor de vulneración múltiple: los derechos fundamentales potencialmente lesionados*

Una de las novedades más importantes que introduce el nuevo RGPD es la necesidad de proteger a los individuos ante la posibilidad de que puedan ser objeto de decisiones basadas únicamente en el tratamiento automatizado de datos y que éstas puedan tener efectos jurídicos o similares.[63] El RGPD no prohíbe la realización de perfiles en general –el *profiling* tiene su mayor desarrollo en el sector comercial, fiscal y laboral–, únicamente prohíbe los perfiles realizados en un contexto determinado y con unas consecuencias también determinadas.[64] El contexto al que alude el RGPD es al de la "ausencia de humanos" en la toma de ciertas decisiones, es decir a que sean las máquinas las que tomen ciertas decisiones basadas en criterios meramente algorítmico. En relación con las consecuencias, éstas tienen que tener efectos jurídicos o similares.[65] Otro límite importante para la elaboración de perfiles viene de-

cuencias de la reidentificación, en lugar de una dicotomía entre datos "identificables" y "no identificables". O. TENE y J. POLONESTKY, "Big Data for All…", cit., pp. 257 y 258.

62 No obstante, tal y como establecen Omer Tene y Jules Polonetsky, el problema es que el modelo de negocio del Big Data es antitético a la minimización de datos, ya que incentiva la recopilación de más datos durante períodos de tiempo más largos. Es decir, está dirigido precisamente a un uso secundario de los datos no anticipado, lo que, según estos dos autores, viene a ser la "joya de la corona" del Big Data. Idem, pp. 259 y 260.

63 Artículo 22.1 RGPD.

64 El RGPD permite la realización de perfiles si ésta es necesaria para la celebración o la ejecución de un contrato; está autorizada por el Derecho de la UE o los Estados miembros, o se basa en el consentimiento explícito del interesado (Art. 22.2).

65 En el considerando 72 del RUE se amplía el concepto de "decisiones con efectos jurídicos o similares" haciendo expresa alusión a decisiones que supongan la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Por el contrario, sí permite la creación de perfiles amparados por el Derecho de la UE y de los Estados miembros, incluso aunque estos perfiles únicamente tengan una finalidad de control fiscal. Solo se fijan dos límites para estos casos: el primero es que se debe proporcionar al interesado información específica al respecto, y el segundo es que debe garantizarse el derecho a la intervención humana.

limitado por la naturaleza de los datos objeto de análisis, ya que no éstos no podrán ser de carácter "sensible", tales como los datos relativos al origen étnico, racial, opiniones políticas, confesiones religiosas, datos relativos a la salud, datos genéticos, etc.[66]

El RGPD define "perfil" como: "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimiento de dicha persona física". Por tanto, la obtención de un perfil a través del análisis de datos masivos puede servir para conocer las diferentes caras de una misma realidad personal, incluso puede hacerse un uso secundario de dichos perfiles, es decir, pueden fijarse perfiles relacionados con los hábitos de consumo alimenticio de una persona que revelen ciertas creencias religiosas o la pertenencia a una comunidad religiosa o ideológica determinada,[67] sin que ni siquiera la persona sea consciente de ello.[68] Además, el perfil –o la clasificación en categorías preestablecidas– no solo "etiqueta" a la persona en un tiempo presente sino que puede condicionarle su futuro sin que ésta pueda hacer prácticamente nada. Cuando los algoritmos hablan de nosotros lo hacen desde el futuro, diciendo qué haremos, qué no haremos, qué seremos o dejaremos de ser. Este hecho sumerge a la sociedad actual en una concepción determinista de la realidad que deja poco margen a la autonomía individual y al libre desarrollo de la personalidad. El determinismo, como explicación de la realidad biológica, ha tenido bastante predicamento dentro del discurso bioético, sobre todo en relación con las denominadas intervenciones genéticas perfectivas o de mejora. Para combatir la fuerza de un argumento que precisamente por su simpleza cala con mucha facilidad, se aplicó en el campo de la bioética de manera analógica el principio argumentativo del "futuro abierto".[69] Este argumento ha

[66] A. GARRIGA, "La elaboración de perfiles…", cit., p. 133.

[67] V. MAYER-SCHÖNBERGER y K. CUKIER, *Big Data*…, cit., pp. 133-136.

[68] Perfiles que permiten clasificar a las personas en diferentes categorías preestablecidas. A. GARRIGA, "La elaboración de perfiles…", cit., p. 130.

[69] Este principio argumentativo fue acuñado por Joel Feinberg para contrarrestar la fuerza condicionante y moduladora –incluso de manera permanente– del entorno cultural y religioso en la personalidad de los niños. Feinberg parte de la idea de que las decisiones de los padres –biológicos o adoptivos– no deberían condicionar a sus hijos a una determinada vida futura, es decir, las decisiones adoptadas libremente por los padres no deben comprometer las

tenido especial acomodo en el debate que se ha generado en relación con las intervenciones genéticas perfectivas y con la clonación humana. Siguiendo con la analogía, podríamos afirmar que el establecimiento del "perfil digital" supone un etiquetado del cual difícilmente podrá zafarse ningún individuo, ya que los perfiles cuentan con el rigor matemático de los algoritmos. De hecho, la creencia de que las personas mentimos o nos enmascaramos en nuestra vida real adoptando posiciones "políticamente correctas" y, por el contrario, nos mostramos como somos en realidad en la vida digital es algo que muchos analistas de datos tienen claro.[70]

De todo lo anterior puede deducirse que el potencial lesionador del establecimiento de perfiles conductuales es múltiple, no se agota en la mera vulneración de la intimidad y la privacidad sino que va más allá, afectando a otros bienes jurídicos tales como la igualdad y el libre desarrollo de la personalidad.[71] Todos ellos amparados por el derecho a la autodeterminación informativa.[72]

El fenómeno relativo a la provocación de "daños múltiples" lo podemos comprobar en relación con el resto de las "tecnologías emergentes" que se caracterizan por implicar o afectar a cuatro cuestiones éticas básicas: igualdad, autonomía, responsabilidad y privacidad/intimidad. La ge-

posibles decisiones libres y futuras de los hijos. Extrapolando esta afirmación al ámbito concreto de la clonación reproductiva, ha de afirmarse que la ignorancia sobre nuestro futuro genético, es decir la no imposición de un genotipo ya conocido y desarrollado, es una parte importante de lo que nos hace entendernos dueños de nuestro futuro, parte de lo que nos permite un libre desarrollo de nuestra personalidad. J. FEINBERG, "The Child`s Right to an Open Future", *Freedom and Fulfilmen Philosophical*, Princeton University Press, Princeton-New Yersey, 1994, pp. 80-82.

[70] Seth Stephens-Davodowitz, analista de datos de Google, sostiene que para conocer a alguien de verdad es mucho más fiable la información que pueda facilitar Google que la que nos puedan facilitar las personas de su entorno más cercano. A través de nuestra actividad en internet –búsquedas, consultas, participación en redes, etc.–, trazamos un perfil de nuestros gustos, preferencias y opiniones que habla por nosotros con más sinceridad y elocuencia que nosotros mismos. S. STEPHENS-DAVODOWITZ, *Everybody Lies. Big Data, New Data and What the Internet Can Tell us About Who We Realy Are*, HarperCollins, New York, 2017.

[71] Martínez de Pisón lleva a cabo un análisis de la jurisprudencia del TC sobre los derechos a la intimidad y a la autodeterminación informativa llegando a la conclusión de que el alto tribunal consolida el carácter personalísimo de los derechos del artículo 18 de la Constitución, es decir, derechos estrechamente relacionados con la dignidad humana y con el libre desarrollo de la personalidad. J. MARTÍNEZ DE PISÓN, "Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo", *Derechos y Libertades*, núm. 37, 2017, pp. 59-62.

[72] Como señala Ana Garriga: "la fijación de perfiles es incompatible con la autodeterminación. El ser humano pasa a ser un mero objeto de información dejando de ser un ser dotado de dignidad humana". A. GARRIGA, *Nuevos retos*…, cit., p. 72.

nética, por su parte, implica una cuestión ética más, la de la integridad/identidad personal, que además sería una característica compartida con la neurociencia y la robótica.[73] Sin embargo esa quinta característica también aparece relacionada con el Big Data. Los cuatro tipos de riesgos destacados anteriormente e identificados como los "riesgos concretos" de la técnica del Big Data: opacidad, inconmensurabilidad, deshumanización y discriminación, suponen una amenaza potencial para estos cinco bienes jurídicos que, a su vez, integran lo que se ha denominado "libre desarrollo de la personalidad".

La perspectiva de los "daños múltiples" que pueden generar las nuevas tecnologías en general y Big Data en particular, nos lleva a adoptar una mirada crítica desde los derechos fundamentales.[74] Por consiguiente, la pregunta lógica que nos debemos plantear ahora es si todos los bienes jurídicos susceptibles de ser lesionados por la aplicación generalizada de Big Data se encuentran protegidos con la normativa actual de manera efectiva, es decir, debemos plantearnos si el "derecho a la autodeterminación informativa" está suficientemente bien garantizado en el contexto jurídico actual.

El derecho a la autodeterminación informativa implica una dimensión de "empoderamiento" del titular de la información personal que en la "realidad digital" puede quedar desdibujada. El ciudadano actual, a través de su actividad en la red, construye su "yo digital" –o "alter ego informático"–, que viene a constituir una parte ineludible de nuestra identidad personal.[75]

---

[73] R. DE ASÍS ROIG, *Una mirada a la robótica desde los derechos humanos*, Cuadernos Bartolomé de las Casas, num. 61, Dykinson, Madrid, 2014, pp. 42-43.

[74] Los derechos humanos constituyen el ineludible marco ético, político y jurídico de referencia para las sociedades contemporáneas, por lo que se convierten en los referentes a tener en cuenta a la hora de analizar el desarrollo tecnológico. Además, tomar como referencia los derechos humanos nos permite adoptar una postura crítica e inconformista, nos permite empatizar con las personas que podrían verse afectadas, y por último, nos dota de unos criterios éticos y jurídicos que nos pueden ayudar a delimitar lo que está justificado y lo que no. R. DE ASÍS ROIG, *Una mirada a la robótica*…cit., pp. 54 y 55.

[75] La "identidad" es la segunda paradoja derivada del Big Data que identifican Neil M. Richards y Jonathan H. King. Estos autores opinan que la influencia digital sobre nuestra identidad es tal que corremos el riesgo de erosionar seriamente la calidad de nuestras democracias. Si el individuo no tiene el poder de decir quién es –"yo soy"–, si son los algoritmos en forma de filtros, cribas y recomendaciones personalizadas los que deciden quiénes somos cada uno de nosotros, entonces nuestras elecciones intelectuales se verán seriamente socavadas y podremos identificarnos pero perderemos nuestra auténtica identidad, al menos tal y como la hemos entendido en el pasado. N. M. RICHARD, J. H. KING, "Three paradoxes of Big Data", cit., p. 44.

La ciudadanía digital no solo necesita el reconocimiento jurídico de su poder de autodeterminación, sino que sobre todo necesita saber cómo gestionarlo, cómo desarrollar y construir de manera consciente su personalidad digital o su identidad digital, lo cual exige el desarrollo de toda una pedagogía social basada fundamentalmente en el respeto a la dignidad humana.

De momento, el RGPD ha dado un paso adelante al invertir la carga de la prueba, exigiendo que sea el responsable del tratamiento de los datos personales el que adopte políticas internas de protección efectiva y aplique medidas encaminadas a cumplir con los principios de "seguridad desde el diseño" y "seguridad por defecto". Dichas medidas podrán consistir en: estar en disposición de demostrar que el consentimiento ha sido prestado conforme al RGPD por el interesado;[76] reducir al máximo el tratamiento de los datos; seudoanonimizar los datos personales lo antes posible con procesos seguros y supervisados de codificación; desarrollar un proceso transparente y facilitar el ejercicio de los derechos que asisten a los titulares de la información.[77] Estas medidas tienen por cometido reforzar la parte "defensiva" de la protección de datos personales, sin embargo la clave de bóveda de la protección de datos sigue hallándose en el "consentimiento informado", como la llave maestra que abre la puerta al tratamiento de los datos personales. El problema es que el modelo de protección datos basado en la responsabilidad, la seguridad y especialmente en el consentimiento informado tenía su razón de ser en un escenario de información escasa, o en cualquier caso de información cuantificable. Con la llegada de Big Data las reglas cambian de tal modo que la obtención del consentimiento informado, tal y como lo hemos concebido hasta la fecha, se torna prácticamente imposible. Informar a las personas adecuadamente para que puedan prestar un consentimiento pleno en la era Big Data supone informar de cuáles son todas las fuentes de las que se van a recabar los datos, de la naturaleza de los datos utilizados, de la fina-

[76] Artículo 7.1 RGPD.

[77] La opción de trasladar el peso de la responsabilidad sobre los datos de los titulares a los responsables del tratamiento parece ser del agrado de algunos estudiosos de los análisis de datos masivos, como es el caso de Viktor Mayer-Schönberger y Kenneth Cukier, ya que sostienen que los responsables del tratamiento son los que mejor saben qué uso quieren darle a los datos, sobre todo porque serán ellos los que tengan que responder legalmente ante un uso indebido de los datos. Es decir, abogan por un cambio de modelo regulatorio pasando de la "privacidad por consentimiento" a la "privacidad por responsabilidad". No obstante, esto conlleva una confianza casi ciega en la buena fe de las empresas bastante cuestionable. V. MAYER-SCHÖNBERGER & K. CUKIER, *Big Data*…, cit., pp. 214 y 215.

lidad o finalidades del tratamiento, etc. Esto es, se trata de dar al ciudadano una información que en muchas ocasiones no van a conocer ni los propios responsables del tratamiento. Además de que en una sociedad en la que la velocidad de la vida se ha acelerado considerablemente, es un tanto ingenuo presumir que el usuario de internet va a dedicar el tiempo necesario a leer y comprender las interminables hojas de información que se requerirían para dar una información adecuada a las exigencias de la legislación. Lo previsible es que el consentimiento se preste de manera automática y mecánica.[78] Por otro lado, tanto con la llegada del internet 2.0 –el internet de las redes sociales–, como con el internet 3.0 –el internet de las cosas–, se ha abierto la puerta a una especie de "consentimiento tácito". Los usuarios de las redes y de dispositivos conectados a internet participan conscientemente de este tráfico de datos, y consienten a través de sus acciones como internautas este flujo constante de información personal.[79]

Este hecho nos obliga a asumir dos verdades inquietantes. La primera es que el ciudadano, en el nuevo contexto de Big Data, pierde irremediablemente parte del control sobre su información personal. La segunda es que los usuarios de internet, en cierto modo, dependemos de la buena voluntad de los responsables y encargados del tratamiento de nuestros datos personales.[80] Estas dos verdades parecen entrar en colisión frontal con el verdadero espíritu del reconocimiento del "derecho a la autodeterminación informativa" en noviembre de 1983 por el Tribunal Constitucional alemán[81] como

[78] Quizá por esto Viktor Mayer-Schönberger y Kenneth Cukier "Para la era de los datos masivos, prevemos un marco muy diferente centrado menos en el consentimiento individual en el momento de la recogida de los datos, y más en hacer responsables a los usuarios de lo que hacen". V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data*…, cit., p. 213.

[79] S. RODOTÁ, *El derecho a tener derechos*, cit., pp. 296-297 y 305.

[80] Independientemente de la "buena voluntad", la práctica de las medidas de transparencia, información y confidencialidad que exige la normativa requieren una buena y sólida formación, compromiso y, sobre todo, tiempo para ponerlo en práctica. Y, como sabemos, el tiempo es oro, por eso estos procedimientos se encuentran protocolizados y automatizados, es decir, que en muchas ocasiones las empresas usuarias de Big Data no tienen el control sobre el propio proceso de análisis de datos masivos. R. HERSCHEL, V. M. MIORI, *Ethics & Big Data*, cit., p. 33.

[81] La Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional alemán 129 delimita, conceptual y jurídicamente, el derecho a la autodeterminación informativa como derecho autónomo y diferenciado del derecho a la intimidad, aun estando reconocido expresamente en el norma constitucional alemana. En la mencionada resolución judicial el Tribunal extrae del derecho al libre desarrollo de la personalidad la facultad de disposición que cada individuo tiene sobre sus propios datos, proyectándose ésta sobre todos los aspectos de su

derecho fundamental de la persona. Este reconocimiento tiene por objeto trasladar el poder de decisión sobre la información personal desde el poder incondicionado del Estado y de los "señores de la información" –operadores económicos privados– hacia el ciudadano. Con ello, nace por tanto una nueva subjetividad basada en la toma de control de la información personal por parte del individuo,[82] y surge a su vez el "cuerpo electrónico", entendido como aquel conjunto de informaciones personales cuyo gobierno debe permanecer siempre bajo el consentimiento de la persona interesada.[83] Si bien la persona debe ser la única hacedora de su propia biografía, la única constructora de su identidad personal, en el ámbito informático la representación de nuestra identidad se construye dentro de los parámetros establecidos por otros, por ejemplo por Google, amo de internet que decide quién, cuánto, cuándo y cómo aparece en sus dominios.[84] Esto da lugar a una "identidad dispersa", ya que las informaciones sobre una misma persona se hallan en bancos de datos diferentes y donde cada uno de ellos recoge partes fragmentadas de la identidad de dicha persona. Además, se trata de una identidad "incognoscible" para el interesado porque muchos de esos bancos de información son de difícil, e incluso imposible, ubicación y acceso.[85]

En cualquier caso, esta concepción dinámica y versátil de la identidad personal[86] pone de manifiesto que los "perfiles" ofrecidos por Big Data se

tratamiento. Se entiende así el derecho a la autodeterminación informativa como la facultad general de disponer de los datos propios. Arranca la tesis argumentativa del tribunal, precisamente en el derecho al libre desarrollo de la personalidad, entendiendo que debe ser el sujeto autónomo, propietario de sus datos personales, el que debe disponer de los mismos con plena libertad. De esta manera, se crea la figura del "habeas data". P. L. MURILLO DE LA CUEVA, "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", cit., pp. 17 y 20. V. BAZÁN, "El habeas data y el derecho a la autodeterminación informativa en perspectiva de derecho comparado", *Revista del Centro de Estudios Constitucionales*, núm. 2, 2005, pp. 90-91.

82 S. RODOTÁ, *El derecho a tener derechos*, cit., p. 240.

83 Afirma Stefano Rodotà que "la autodeterminación en la vida y en el cuerpo representa el punto más álgido y fuerte de la libertad existencial". Idem, p. 231.

84 Idem, pp. 277-279.

85 ÍIem, p. 293.

86 Rodotá sigue el paradigma de Montaigne que entiende la identidad personal como una construcción permanente. Una identidad permanente y también múltiple, ya que en el especio virtual podemos ser una o muchas identidades. De ahí que haga referencia al paradigma denominado "Zelig" haciendo alusión al personaje que da nombre a la película de Woody Allen. La personalidad múltiple es otra de las singularidades del mundo virtual. Idem, pp. 277 y ss.

han convertido en el nuevo "lecho de Procusto"[87] con esa obsesión enfermiza de encajar en un molde restringido, limitado y estático la compleja realidad individual. La identidad personal, como constructo individual y libre que nos otorga un lugar en el mundo, constituye la libertad positiva o la libertad de autodeterminación de la que goza el sujeto sobre su propio cuerpo. El individuo es soberano tanto en su realidad corporal como en su realidad mental, espacios en los que puede ejercer su libertad de autodeterminación. Dentro de su realidad mental el sujeto titular del derecho a la integridad moral y psicológica puede determinar tanto los contenidos de ésta como sus propios límites, a través del ejercicio de una pléyade de libertades públicas como la libertad ideológica, religiosa, de culto, de expresión, de comunicación, artística y científica. El reconocimiento y garantía de estas libertades tiene una doble finalidad. Por un lado, pretende la abstención –prácticamente en términos absolutos– de cualquier tipo de intervención o injerencia de los poderes públicos en estas esferas estrictamente privadas. Por otro lado, busca que el individuo pueda desarrollar libremente su personalidad, es decir, que se comprenda como un ser autónomo y, por consiguiente, como un ser digno.[88] Sin embargo, cuando nos adentramos en el mundo digital, la identidad se encuentra condicionada por dos factores. Uno es temporal y se proyecta tanto hacia el futuro como hacia el pasado. Hacia el futuro porque, como ya se ha advertido, la elaboración de algunos perfiles, como pueden ser los perfiles ideológicos, religiosos, sanitarios, etc., pueden condicionan seriamente nuestro libre desarrollo de la personalidad, cerrándonos el paso a un futuro libremente decidido, plegando así nuestro libre albedrío a la tiranía de los algoritmos que pretenden convertirnos en moldes intercambiables en el mercado digital[89]; y hacia el pasado, porque la memoria digital es infinita. Nuestra narrativa personal, la narración biológica de nuestras vidas, es

[87] Procusto es un personaje de la mitología griega propietario de una casa en la que daba hospedaje a los viajeros solitarios. Allí los invitaba a tumbarse en una cama de hierro donde, mientras el viajero dormía, lo ataba a las cuatro esquinas del lecho. Si la víctima era alta procedía a serrarle las partes del cuerpo que le sobresalían de la cama, y si su víctima era baja le estiraba las extremidades. Nadie se adaptaba a las dimensiones de su cama porque el lecho de Procusto era ajustable.

[88] V. MORENTE, *Nuevos retos biotecnológicos para los derechos fundamentales*, Comares, Granada, 2014, pp. 310-311.

[89] Partiendo de la idea de Byung-Chul Han de entender la sociedad actual o "sociedad de la transparencia", como un "mercado en el que se exponen, venden y consumen intimidades", podríamos afirmar que internet nos ofrece un mundo en el que se exponen, venden y consumen "identidades". Véase B. C. HAN, *La sociedad de la transparencia*, cit., p. 68.

dinámica, selectiva y figurativa, es decir nuestro cerebro procede a seleccionar aquello que entiende memorable, lo magnifica, lo distorsiona, etc., ajusta nuestro pasado a nuestra identidad presente. Sin embargo, la memoria digital es invariable y puede ser incluso tiránica, ya que el olvido es fundamental para la construcción de nuestra identidad.[90]

El segundo factor condicionante de la identidad personal digital es el del "relato simultáneo". Como ya hemos advertido, la identidad digital no solo depende de nuestra narración, de nuestras acciones, omisiones o interacciones con otras personas, sino que es el resultado de un diálogo simultáneo y permanente que escapa a nuestro control. Esto se ve claramente en las redes sociales, cuando se puede conocer la identidad digital de una persona a través del perfil de otra, es decir, por derivación. Este diálogo permanente de construcción de identidades digitales se desarrolla en lo que se ha denominado "identidad digital aumentada" que "potencia y proyecta las experiencias de los individuos y que permite transmitir pensamientos, imágenes y contenidos de forma instantánea a través de diferentes redes relacionales interconectadas entre sí".[91]

A la luz de lo dicho hasta aquí, y sin ánimo derrotista, podríamos concluir que, al menos en lo referente a nuestra "vida digital", no estamos en un momento histórico de conquistas para la dignidad humana, sino todo lo contrario. Parece que las nuevas tecnologías nos hurtan cada vez más deprisa espacios que hasta la fecha creíamos conquistados por los derechos fundamentales. En una sociedad que se cree más libre que ninguna otra nos encontramos más encadenados que nunca. ¿Cómo vamos a mantener el espacio conquistado por los derechos fundamentales ante este tsunami informático? Quizá lo primero que haya que asumir sea precisamente la pérdida paulatina de la autogestión de ciertos espacios, al menos como lo hemos entendido hasta ahora. Esta pérdida de autogestión se proyecta sobre nuestra intimidad, privacidad y nuestro libre desarrollo de la personalidad en pos de una "vida digital" inserta en una comunidad de identidades poliédricas y participadas, donde seguramente surgirán nuevas formas de discriminación basadas en perfiles algorítmicos que gozarán del rigor matemático. Nos encontramos pues, ante potencial una nueva clasificación social, e incluso en el

[90] J. A. BURKELL, "Remembering me: Big Data, individual identity and the psychological necessity of forgetting", *Ethics and Information Techonology*, num. 18, 2016, p. 18.

[91] M. PÉREZ SUBÍAS, "Identidad digital", *Telos. Cuadernos de Comunicación e innovación*. Fundación Telefónica, 2012, p. 2 disponible en *www.telos.es* (consultado en julio de 2017).

peor de los casos, ante nuevas estigmatizaciones sociales. Quizá ni siquiera podamos apelar a una nueva hermenéutica de los derechos fundamentales con la finalidad de adaptarlos a las exigencias de la sociedad informática, y lo que nos quede únicamente sea asumir la pérdida "consentida" y "consciente", total o parcial, de algunos espacios que creíamos conquistados.

2.2.3. El consentimiento condicionado al interés general: el modelo de consentimiento opt-out en el ámbito de la sanidad pública

Si bien es cierto que el RGPD ha venido a consolidar en el contexto europeo una cultura de protección de datos proactiva, basada en la autonomía y fundamentalmente en la responsabilidad positiva de los usuarios de los datos, no es menos cierto que el nuevo escenario digital delimitado por el Big Data y el resto de tecnologías disruptivas dificultan este propósito. Como hemos podido comprobar en el epígrafe anterior, el consentimiento informado no es pleno, por lo que se produce una manifiesta "pérdida de soberanía" sobre nuestra información personal. No obstante, esta pérdida de soberanía o de poder de autodeterminación sobre nuestra información personal no debe juzgarse negativamente desde todos los ámbitos, pues hay espacios en los que el consentimiento no solo se ve limitado sino que "debe ser" limitado.[92]

La aplicación de Big Data en el ámbito sanitario,[93] aunque aún se encuentra en ciernes, va aumentando paulatinamente gracias a diversas iniciativas que van consolidando una efectiva y plena implementación de esta

[92] Si partimos de la idea que manifestó Tim Kelsey en 2015 como director de pacientes e información del NHS británico, en la que entiende la aplicación de Big Data en el ámbito de la salud como un "imperativo moral", la pérdida de un control absoluto por parte del paciente en relación con su información sanitaria estaría justificada en pro de un mayor y mejor desarrollo de la ciencia médica, que tiene una innegable vocación de servicio público.

[93] El Informe sobre Big Data y Salud Digital elaborado por la Fundación Vodafone España y Red.es destaca los ámbitos en los que Big Data tiene mucho que aportar al sector sanitario: ayuda a transformar los datos en conocimiento; mejora el aprovechamiento de la información; provoca un salto cuantitativo y cualitativo en la investigación clínica; genera nuevos instrumentos de conocimiento y formación para los profesionales de la salud; ayuda en la promoción del "autocuidado de la salud" empoderando a los pacientes. Véase "Informe sobre Big Data y Salud Digital", ob. cit., p. 28. El Comité Internacional de Bioética (IBC) de la UNESCO en su reciente Informe sobre el Big Data en salud de 2017, señala en el mismo sentido que el Big Data puede considerarse ya un bien común de la humanidad. Los avances y las nuevas oportunidades proporcionadas por la ciencia y la tecnología podrían ayudar a reducir y no profundizar las desigualdades que impiden a muchos seres humanos disfrutar del más alto nivel posible de salud, tanto a nivel nacional como internacional. Véase

nueva técnica en el ámbito de la sanidad.[94] Es precisamente en este ámbito en el que la regulación sobre el tratamiento de los datos personales es menos exigente que en el resto. En pos de un mayor y mejor desarrollo de la investigación científica en el espacio europeo, el RGPD flexibiliza ciertos aspectos del tratamiento de los datos a pesar de que se trata de datos sensibles. Esta flexibilización se comprueba sobre todo en la obtención del consentimiento informado. El RGPD asume que con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de la recogida de dichos datos. Por consiguiente, se permite la manifestación de un consentimiento para determinados ámbitos de investigación científica, siempre que se respeten las normas éticas previstas para este ámbito. La única limitación es que los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.[95]

Además en las excepciones previstas a la regla general, que es la obtención del consentimiento tipo –manifestación de la voluntad libre, específica, informada e inequívoca por la que el interesado acepta el tratamiento–, el RGPD contempla la posibilidad de tratar datos relativos a la salud sin la previa obtención del consentimiento cuando el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, y cuando el tratamiento tiene como finalidad la investigación científica o la realización de estadísticas.[96] No obstante, el RGPD deja un margen de decisión a los Estados

"Informe sobre Big Data y salud digital" de septiembre de 2017 (*http://unesdoc.unesco.org/images/0024/002487/248724e.pdf*).

[94] La utilidad de la aplicación del Big Data en el ámbito sanitario es de un inmenso valor, sobre todo en relación con los siguientes sectores: genómica; investigación clínica; epidemiología; seguimiento de enfermos crónicos; operativa clínica; farmacología, etc. Véase "Informe sobre Big Data y Salud Digital", ob. cit., pp. 29-34. Si bien es cierto que las ventajas de la aplicación de Big Data al ámbito sanitario son muchas y my prometedoras, no es menos ciertos que esta utilidad también supone un recurso muy valioso para los que deseen explotarlo con fines lucrativos, como las compañías farmacéuticas y de seguros. M. FULLER, "Big Data: New Science…", cit., p. 571.

[95] Considerando 33 del Reglamento de la Unión Europea sobre Protección de Datos.

[96] Artículos 9 i) y j) del RGPD. En el considerando (54) determina el Reglamento que "el tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y las libertades de las personas físicas. (…) Este tratamiento de datos relativos a la salud por razones de interés público –se refiere la norma al tratamiento de datos sensibles sin el consen-

miembros al permitirles introducir condiciones adicionales, incluso limitaciones, con respecto al tratamiento de los datos genéticos, datos biométricos o datos relativos a la salud.[97]

Tanto la salud pública como la investigación sanitaria pública encuentran su razón de ser en el interés general, de ahí que el Reglamento insista en esta cuestión en reiteradas ocasiones.[98] Precisamente porque se trata de cuestiones cuya fundamentación se encuentra en el interés general podría estar justificada la aplicación de un modelo de consentimiento menos rígido, como es el modelo de consentimiento "opt-out" u opción salir.[99] El problema es que el RGPD parece suprimir el "consentimiento presunto", es decir, que el consentimiento informado habrá de manifestarse expresamente. Solo a través de este modelo de consentimiento expreso, la información personal podrá entrar dentro de un proceso de tratamiento automatizado de datos personales lícito, que incluso en el caso de los datos sanitarios debe estar formalizada por escrito.

Lo que aquí se propone, aunque no es la posición mayoritaria,[100] es que en el espacio europeo sea el modelo contrario el que opere como regla gene-

timiento del interesado–, no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".

97 Artículo 9.4 del RGPD.

98 En este sentido, Federico de Montalvo afirma que resulta un contrasentido mantener una posición –en relación con el consentimiento informado en el ámbito sanitario– que únicamente atienda a la dimensión individual o subjetiva, cuando el modelo tiene rasgos esenciales de comunitarismo. Resolver nuestros problemas sanitarios a cargo de los presupuestos públicos nos exige también de los ciudadanos un ejercicio de responsabilidad y ésta se manifiesta en el contexto actual del avance de la tecnología en el deber moral –que no jurídico como afirma el autor– de compartir los datos para que, aquellos otros que no han logrado tan fácilmente la curación, puedan obtenerla. Véase F. DE MONTALVO, "¿Puede la máquina sustituir al hombre?…", cit. (versión online consultada en octubre de 2018).

99 Omer Tene y Jules Polonestky afirman que cuando los beneficios derivados del tratamiento de los datos superen a los riesgos derivados para la privacidad del sujeto fuente, debe abogarse por el tratamiento de los datos, incluso aunque el responsable del tratamiento no cuente con el consentimiento de los afectados. Es decir, apuestan por un uso secundario de los datos a través de un "consentimiento presunto", o modelo de consentimiento opt-out, que podría constituir la regla general para tratamiento de datos relacionado con la salud pública. O. TENE, J. POLONESTKY, "Privacy in the age of Big Data: a time for big decisions", *Stanford Law Review*, num. 64 vol. 63, 2012, pp. 67 y ss. (revista on line consultada en julio de 2018).

100 Omer Tene y Jules Polonestky abogan también por el modelo de consentimiento presunto o modelo "opt-out", afirmando que la función del consentimiento debería ser demarcada de acuerdo con las elecciones normativas realizadas por los responsables de las políticas con respecto a usos prospectivos de datos personales. Ambos autores afirman que en

ral en el sector de la salud pública y de la investigación sanitaria financiada con fondos públicos. Es decir, que el "consentimiento tipo" en el ámbito sanitario sea el modelo opt-out, o la manifestación expresa de querer retirar la información personal del tratamiento de datos en el que ha sido incluida por defecto. Este cambio de modelo ya fue implementado en España en el ámbito de las donaciones de órganos y ha resultado todo un éxito, ya que el número de donaciones en España es el más alto del mundo.[101] Además, ha de tenerse en cuenta que el sector sanitario está regulado y limitado por el "deber de secreto", base fundamental de la relación de confidencialidad entre el personal sanitario, y el paciente y que viene a reforzar la seguridad en el tratamiento de los datos personales.

En su versión más restrictiva, la regla del consentimiento "opt-out", o consentimiento presunto, podría limitarse de tal modo que no fuese aplicable a aquellas investigaciones clínicas o biomédicas que, aunque tiendan a satisfacer un interés general, tengan una clara finalidad lucrativa de carácter privado. Esta opción obliga a mantener el modelo tradicional del consentimiento expreso, ya que la excepción quedaría justificada solo si se cumplen dos requisitos: el primero es el interés general y el segundo la previsión de un beneficio exclusivamente público o incluso la gratuidad. Si entendemos el consentimiento presunto en el ámbito sanitario como la clave para obtener un "patrimonio común" del que se beneficia la sociedad en su conjunto, parece lógico exigir ambos requisitos con la finalidad de proteger un bien público –el repositorio de informaciones sanitarias y clínicas de toda la población– que podría ser aprovechado para satisfacer intereses económicos de carácter privado. El problema es que la mayoría de los ensayos clínicos de los que conocen los Comités de Ética de la investigación de los Hospitales públicos españoles son promovidos y financiados por la industria farmacéutica. Y si bien la empresa farmacéutica busca un beneficio económico en cada uno de sus proyectos de investigación, no es menos cierto que si estos proyectos concluyen satisfactoriamente repercuten positivamente en la sociedad en general.

Por su parte, en su versión más amplia, el "modelo de consentimiento presunto" en el ámbito sanitario podría apoyarse solo en el criterio del in-

---

algunos casos el consentimiento ni siquiera debería ser requerido, mientras que en otros, el consentimiento debe suponerse sujeto a un "derecho de rechazo" u "opción salir". O. TENE, J. POLONESTKY, "Big Data for All…", cit., pp. 262 Y 263.

[101] España lleva 26 años siendo líder mundial de donaciones de órganos según el Ministerio de Sanidad. *http://www.msssi.gob.es/gabinete/notasPrensa.do?id=4189* (06/07/2018).

terés general, posibilitando así un uso privativo de un "patrimonio común" como es la información sanitaria. Es decir, las empresas privadas podrían lucrarse de dicho patrimonio público, ya que si bien la industria sanitaria busca maximizar su beneficio económico, no es menos cierto que sus resultados –bienes y servicios sanitarios– pueden repercutir muy positivamente en la calidad sanitaria de la sociedad en su conjunto.

La pregunta que deberíamos plantearnos ahora sería la siguiente: ¿Qué modelo de "consentimiento presunto", restrictivo o amplio, garantiza mejor los derechos fundamentales?

En el modelo restrictivo apoyado en los dos criterios señalados anteriormente –interés general y gratuidad–, se cierra la posibilidad de un lucro de carácter privado a partir de un bien público –información sanitaria común–, aunque también se podría estar limitando un desarrollo más rápido y efectivo de la investigación clínica y biomédica. Podríamos afirmar que en este modelo primaría la protección del derecho a la intimidad, la protección de datos personales y el libre desarrollo de la personalidad frente al derecho a la salud, que en buena medida depende del desarrollo satisfactorio de las investigaciones científicas y médicas, ya sean éstas públicas o privadas. En un país como España, donde la financiación pública destinada a la investigación científica es cada vez más exigua, la aplicación de un modelo restringido de consentimiento presunto en el ámbito sanitario, podría llevarnos a estrangular el desarrollo de la investigación científica y médica, ya que ante la ausencia de lo público, este espacio ha sido ocupado por la industria farmacéutica, que es la que promueve y financia buena parte de los proyectos de investigación.

Por su parte, en el modelo amplio de consentimiento presunto se abandonan las ideas de beneficio público y gratuidad, apostando por un uso público-privado de la información sanitaria en pro de conseguir mejores diagnósticos y mejores tratamientos para la sociedad en general. En este modelo se pierde cierto poder de autodeterminación individual, y se asume el riesgo de un uso privado de la información sanitaria con la idea de potenciar el derecho a la salud de la población en general. En cualquier caso, el modelo amplio de consentimiento presunto en el ámbito sanitario, debería ir precedido de una "pedagogía social", a través de la cual informar a la sociedad de las utilidades de estudiar y analizar la información sanitaria en su conjunto. Del mismo modo que en España ha calado la cultura de la donación de órganos desinteresada y presunta, esta pedagogía de la "donación de información

sanitaria" debería ayudar a que la sociedad tome consciencia de la necesidad de promover un flujo informativo sanitario que permita la consecución de mejores diagnósticos, e incluso de mejores tratamientos médicos. Es decir, debería generarse un caldo de cultivo social apropiado en el que germine la cultura de la donación presunta de datos sanitarios y en el que se propicie un flujo constante de informaciones sanitarias del que todos podríamos beneficiarnos.

3. ALGUNAS CONCLUSIONES

La tecnología del Big Data es el arte de analizar datos masivos con la finalidad de identificar patrones conductuales. Se trata en realidad de "la nueva alquimia", pues a través de la combinación y aleación de datos masivos, proporciona un material muy preciado y codiciado, como son los perfiles conductuales. Dichos perfiles se basan en correlaciones que vienen a explicar el "qué" –a veces de manera espuria y otras veces incluso de manera errónea– pero no el "por qué" de las acciones humanas.

Es innegable que la formulación de estas "predicciones", a través del perfilado conductual, ha demostrado ser una herramienta muy útil en muchos sectores económicos, sin embargo un análisis meramente económico del Big Data sería realmente pobre. En el presente trabajo se han intentado destacar los riesgos a los que nos enfrentamos como sociedad digital. Para ello, nos hemos valido, a modo de analogía, del esquema crítico-analítico propuesto por Ulrich Beck y denominado por él mismo como "el modelo de los riesgos civilizatorios". Gracias a este patrón de análisis sociológico podemos concluir que de la aplicación de algunas técnicas disruptivas, entre las que se encuentra el Big Data, se derivan una serie de riesgos de carácter futuro, invisible, universal y potencialmente discriminador. Y, como no podía ser de otro modo, los riesgos sociológicos tienen su vertiente ético-jurídica, manifestada en cuatro tipos de riesgos: el riesgo de la opacidad, el riesgo de la inconmensurabilidad, el riesgo de la deshumanización, y, por último, el riesgo de la discriminación.

Estos riesgos suponen en realidad nuevos desafíos a los derechos fundamentales, siendo este uno de los motivos por los que la Unión Europea procedió a aprobar el Reglamento General de Protección de Datos en abril de 2016, con la intención de proporcionar una mayor y mejor protección a nuestra privacidad. Este nuevo Reglamento, además de homogeneizar la

política de protección de datos en el espacio europeo, ha venido a consolidar una filosofía proactiva en la protección de datos personales, basándose para ello en dos principios fundamentales: seguridad desde el diseño y seguridad por defecto. Además, el RGPD por una parte introduce nuevos derechos como el derecho al olvido, el derecho a la limitación del uso de los datos y el derecho a la portabilidad de la información; y por otra parte refuerza algunos derechos ya consagrados como el derecho a no ser objeto de una decisión con consecuencias jurídicas o similares que haya sido adoptada sin la intervención de un humano. Estas decisiones podrían tomarse como consecuencia de lo que se ha denominado el "perfilado" personal o grupal, que en realidad supone el etiquetado de una de una persona, no solo en el tiempo presente, sino también en el futuro. Se trata de una clasificación presente con proyección futura que no deja margen al libre desarrollo de la personalidad, por lo que podríamos afirmar que se trata de una nueva manera de "determinismo". Esto pone de manifiesto que el potencial lesionador de la aplicación del perfilado es múltiple, es decir no se agota en la mera vulneración de la intimidad y la privacidad sino que va más allá, afectando a otros bienes jurídicos tales como la igualdad y el libre desarrollo de la personalidad.

El problema es que para hacer frente a una fuente de lesiones potenciales y múltiples sería necesario empoderar aún más al individuo, sin embargo en la sociedad digital la manifestación de un consentimiento voluntario, libre, específico e inequívoco, es verdaderamente cuestionable, ya que en muchos casos el consentimiento se presta tácitamente. Y siendo cierto que el consentimiento presunto puede poner en riesgo algunos derechos fundamentales de los usuarios de internet, no es menos cierto que en ámbitos como el sanitario puede ser incluso beneficioso para la población en su conjunto. Aquí se ha intentado justificar la necesidad de implementar un modelo de consentimiento presunto, o modelo "opt-out", en el ámbito de la investigación científica y sanitaria. Este modelo de consentimiento podría aplicarse o bien de manera restrictiva debiendo atender a dos criterios: en primer lugar que se trate de investigación dirigida a satisfacer un interés general; y, en segundo lugar, que no tenga un ánimo de lucro de carácter privado. O bien de manera amplia, si el modelo de consentimiento presunto estuviera sujeto únicamente al criterio del interés general, en cuyo caso se posibilita el uso privativo de un bien público como es la información sanitaria. En ambos casos habrá de llevarse a cabo un juicio ponderado de

los derechos fundamentales que se pueden ver afectados, así como de las utilidades y ventajas reales de las que se puede beneficiar la ciudadanía en general.

VANESA MORENTE PARRA
Universidad Pontificia Comillas - ICADE
c/ Alberto Aguilera, 23
28015 Madrid
e-mail: vmorente@comillas.edu

ISSN: 1133-0937
DOI: 10.14679/1216