Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales

Lorenzo Cotino Hueso*
Universidad de Valencia (España)
cotino@uv.es

Big Data and Artificial Intelligence. An Approach from a Legal Point of View about Fundamental Rights

Resumen: El estudio alerta de algunos peligros del big data y la inteligencia artificial: los datos masivos y los algoritmos no son objetivos, pueden tener importantes sesgos o "incrustados" valores contrarios a los constitucionales. Frente a la discriminación, brecha y sesgo algorítmicos, se plantean garantías en el ámbito del análisis de impacto de privacidad o la no discriminación por defecto y en el diseño. Se hace referencia a la pérdida de la esfera pública y la postverdad, así como a la libertad de expresión de las máquinas. También se intenta fundamentar un derecho a la "transparencia algorítmica" o se plantean cuestiones por el uso del Big data en inteligencia artificial en la aplicación de la ley y la justicia. Se afirma la superación del consentimiento como garantía efectiva de la privacidad, las dificultades de proyectar los principios de la protección de datos o los derechos ARCO o la importancia de la anonimización de datos.

Palabras clave: big data, datos masivos, inteligencia artificial, derechos fundamentales, protección de datos

Abstract: Some dangers of big data and artificial intelligence are warned: data and non-objective algorithms can have important biases or "embedded" values. Guarantees against discrimination and "algorithmic bias" are affirmed, in the scope of privacy impact assessment or non-discrimination by default and by design. Some reflections are made on the massive personalization of information, the loss of the public sphere and the post-truth, as well as the freedom of expression of machines. Also a right to "algorithmic transparency" is intended to affirm and base. Different questions are exposed about the use of Big Data and artificial intelligence in law enforcement and justice. Finally, about privacy and data protection, it is stated that the guarantee of consent is outdated and ineffective and the difficulties of projecting the principles of data protection, as well as the importance and problems of anonymization are also affirmed.

Keywords: big data, massive data, artificial intelligence, fundamental rights, data protection

ISSN 1989-7022

1. Qué es, de dónde viene y para qué

1.1. De qué hablamos cuando hablamos del big data o los datos masivos y su potencial económico

La expresión "big data" trae causa del trabajo de Schönberger y Cukier (2013 a). En español se utiliza la expresión inglesa "big data", también "macrodatos" (Parlamento Europeo, 2017) y no tanto la de "datos masivos". Se habla de las "V" (Gartner, 2012): volumen, variedad, velocidad y valor, a las que se añaden entre otras, la veracidad (Puyol, 2014, 488). Se hace referencia al carácter "big", grande o masivo de los datos para referir al Volumen, esto es, a cantidades de datos ingentes, de magnitud casi tan inabarcable a la mente humana como la grandeza del espacio. Y tales datos masivos también pueden tener la V por su "Variedad" de fuentes y naturaleza. También se destaca como tercera "V" la gran Velocidad en la gestión y actualización de los datos. Los datos a los que se hace referencia pueden estar estructurados, no estructurados o parcialmente. No obstante, más

* www.cotino.es El presente estudio es producto de investigación en el marco del Grupo en Derecho Público y TIC, de la Universidad Católica de Colombia. Dentro de la investigación "Derecho y Big Data" (2017-2018). Asimismo, se realiza en el marco del Proyecto español del Ministerio de Economía "El avance del Gobierno Abierto. Régimen jurídico constitucional de la implantación de políticas de transparencia, acceso a la información, datos abiertos, colaboración y participación especialmente a través de las TIC y del gobierno electrónico" DER2015-65810-PÁG.

Received: 05/05/2017
Accepted: 15/05/2017

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 131-150

allá de la cantidad o estructura, se destaca con el término big data elementos como la V del gran Valor potencial presente y especialmente futuro. También es nota diferencial de los datos masivos que éstos no pueden ser manipulados, analizados, procesados, con mecanismos o procesos tradicionales.

El gran reto de los datos masivos es la captación, gestión y tratamiento para agregar valor a grandes volúmenes de datos poco utilizados o inaccesibles hasta la fecha, todo ello para aportar y descubrir un conocimiento hasta ahora oculto. Entre otros, Boyd y Crawford (2011, 6) subrayan que el Big Data no sólo se refiere a grandes conjuntos de datos y las herramientas y procedimientos utilizados para manipular y analizar ellos, sino también a un giro en el pensamiento computacional y la investigación (siguen a Burkholder, 1992). Así como Ford cambió la forma en que hicimos coches -y luego se transformó trabajo- el Big Data va a cambiar toda la teoría social (Latour, 2009, p. 9) al automatizar tanto el objeto como el procedimiento del conocimiento. Y precisamente por ello, el big data en muy buena medida está conectado con la inteligencia artificial (IA) cuando los sistemas computacionales son capaces de tratar, aprender, resolver problemas y tomar decisiones a partir de los grandes datos bajo un cambio de paradigma que automatiza tanto el objeto (los datos). Se aplican algoritmos, redes neuronales artificiales y patrones de razonamiento, en principio, similares a los humanos (Nilsson Nils, 1980). En esta dirección, el Parlamento Europeo (2017, Considerando b) recuerda que con los macrodatos en algunos casos se capacitan "dispositivos de inteligencia artificial "como redes neuronales y modelos estadísticos con el fin de predecir algunos acontecimientos y comportamientos".

No es difícil prever la importancia económica del big data. Así por ejemplo y para Europa, algunos estudios (Demoseuropa, 2013) ya señalaban que en 2020 la combinación del big data y el open data, especialmente el primero implicará un crecimiento de 230 mil millones de euros, un 1,9% adicional al PIB. Ello implica un incremento adicional del PIB de un 23% en comercio, 22% en industria, 13% en financias y seguros, un 13% en Administración, un 6% en sector TIC y un 5% en sanidad y servicios sociales. Se afirma que un 50% de la economía europea queda afectada por el big data y que afecta a un crecimiento de un 5-6% de su eficiencia (Smart-Comisión Europea, 2013). Más recientemente se afirma que "el sector de los macrodatos está creciendo a un ritmo del 40% anual, siete veces más rápidamente que el del mercado de las tecnologías de la información" (Parlamento Europeo, 2017, Considerando k).

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

1.2. De dónde proceden los datos masivos y todo lo imaginable que se puede hacer con ellos

Los grandes datos son generados por humanos, también biométricamente, producidos máquina a máquina, producto de grandes transacciones o del uso de la web y redes sociales (Sunil Soares, 2012). Billones de *whatssaps*, correos electrónicos, contenidos en Facebook, Twitter, búsquedas en Google, vídeos en Youtube. Resulta muy sugestivo acceder a www.internetlivestats.com para apreciar las magnitudes. Los datos masivos se generan por la navegación en internet, las comunicaciones del internet de las cosas, comunicaciones entre máquinas, industrias, estaciones meteorológicas, etc. por lo general vinculadas a medidores y sensores de temperatura, luz, altura, presión, sonido, localización, GPS, así como en el entorno de tecnologías RFID, wifi o bluetooth. A sumar a los datos biométricos, normalmente vinculados al ámbito de seguridad pero también de sanidad (escáneres de retina, de huellas digitales, o lectores de cadenas de ADN, monitoreos médicos de todo tipo, etc.).

Qué se hace con datos, en palabras de (Martínez, 2014, 3) a partir del clásico de Mayer-Schönberger "es un territorio abierto a la imaginación"; se trata de una "estadística del todo" por el que el científico puede analizar todos los datos, eliminando el sesgo de la elección de una muestra. Además, merced a las posibilidades de tratamiento, se combinan datos como el químico que aleatoriamente va tomando muestras por doquier. Frente a la contrastación de una hipótesis a partir de los datos, se descubren correlaciones sin conocer previamente la causa. Así sucede al probar casi aleatoriamente la posible correlación entre datos en principio totalmente distantes (¿Compra distintos alimentos la gente en función del estado del clima? ¿Cómo influye el embarazo en las decisiones de consumo? ¿Sería posible ofrecer seguros de salud en función de las búsquedas en Google o del análisis de las preferencias alimentarias manifestadas por los usuarios y por sus redes de amigos en espacios sociales de internet?).

Así las cosas, gracias al big data y la inteligencia artificial se permite generar patrones dinámicos de tendencias de futuro: la predictibilidad y el apoyo en la toma de decisiones. Se puede conocer mejor al cliente, al mercado, personalizar los productos y servicios, mejorar y agilizar la toma de decisiones, prever el comportamiento (AEPD-ISMS, 2017, 6-7). El big data y la inteligencia artificial se proyectan en los sectores público y privado al ámbito empresarial, de recursos humanos, de

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

marketing, de consumo, de comercio, de transporte, de sanidad, educación, y un largo etcétera. Del lado de las ventajas, más allá de la perspectiva de intereses privados, sin duda pueden repercutir en ámbitos de la asistencia sanitaria, la lucha contra el cambio climático, la reducción del consumo energético, la mejora de la seguridad en el transporte y la posibilidad de establecer ciudades inteligentes, mejorando, así, la optimización y eficiencia de las empresas y contribuyendo a una mejora de las condiciones laborales y a la detección y la lucha contra el fraude; y que los macrodatos pueden ofrecer una ventaja competitiva para los procesos de toma de decisiones (Parlamento Europeo, 2017, Considerando h).

En cualquier caso, uno de los mayores retos es disponer de personas adecuadas y formadas para analizar y explotar los datos, esto es, convertir una gran cantidad de datos en decisiones, estrategias y mejores experiencias para los consumidores.

2. Algunas cautelas que plantea el big data y la necesidad de abordarlo ética y jurídicamente. Una ética sólida frente a errores masivos y estupidez artificial.

Como ya señalasen Boyd y Crawford (2011), los números no hablan por sí mismo; las afirmaciones de objetividad y precisión son engañosas dado que todos los investigadores son intérpretes de datos y siempre hay un proceso de "limpieza de datos" inherentemente subjetivo. También apuntan que con los datos masivos, también hay errores de datos masivos. Los datos de internet, en razón de interrupciones y pérdidas son a menudo poco fiables, y los errores y lagunas se hacen también masivos. También se ha criticado lo más grande no necesariamente es mejor.

Nuestro uso tecnológico genera datos vaporosos ("data fumes", Thatcher, 2014, 1770) con todas sus limitaciones, sesgos y manipulaciones. Se ha llegado a hablar de "Weapons of math destruction" (O'Neil, 2016). Como señala Surden, lejos del "manto de objetividad de la tecnología", los sistemas tecnológicos pueden tener valores sociales "incrustados" o embebidos en su diseño y que éstos sean contrarios a la igualdad, principios constitucionales y derechos humanos (Surden, 2017, 2). La "baja calidad" de los datos o los procedimientos:

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

> *"podrían dar lugar a algoritmos sesgados, correlaciones falsas, errores, una subestimación de las repercusiones éticas, sociales y legales, el riesgo de utilización de los datos con fines discriminatorios o fraudulentos y la marginación del papel de los seres humanos en esos procesos, lo que puede traducirse en procedimientos deficientes de toma de decisiones con repercusiones negativas en las vidas y oportunidades de los ciudadanos, en particular los grupos marginalizados, así como generar un impacto negativo en las sociedades y empresas" (Parlamento Europeo, 2017, Considerando m). "[L]a información revelada por los análisis de los macrodatos no ofrece una visión general objetiva e imparcial de ninguna materia y que es tan fiable como lo permitan los datos subyacentes (Parlamento Europeo, 2017, Cons. General 2).*

Richards y King (2013, 41) afirman importantes cautelas y una necesaria visión crítica frente a los "grandes evangelistas" del big data, esto es, los que prometen que los grandes datos pueden mejorar la toma de decisiones por las mejores predicciones en áreas que van desde la admisión a la universidad, los servicios y políticas médicas, de seguridad nacional o prevención del delito. Afirman la paradoja de la transparencia, por la que mientras que con los datos masivos se accede invasivamente a información privada, los resultados de estos tratamientos están casi completamente rodeadas de secreto legal e industrial. Subrayan especialmente la paradoja que implica que un futuro casi milagroso y de transformación social sea al fin y al cabo un privilegio que queda en manos del gobierno y de grandes empresas, a costa de los ciudadanos, y todo ello en el contraste de los riesgos de la identidad individual y colectiva.

Todo ello puede llevarnos a la "dictadura de los datos" (Cukier y Mayer-Schönberger, 2013 b), o como he señalado, a errores masivos o a una estupidez artificial, que sería, eso sí, muy humana.

Así las cosas y como reacción frente a estos riesgos se afirma la idea de una "responsabilidad algorítmica, bajo la idea de que las "normas científicas y éticas estrictas, son fundamentales" (Parlamento Europeo, 2017, Consideración 2), la necesidad de un "marco ético común sólido" (20), al igual que se apela a "las normas éticas más elevadas" (32) especialmente cuando se usen los macrodatos en la aplicación de la ley.

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 131-150

3. La necesaria aproximación jurídica sobre los derechos fundamentales y nuevos enfoques

La ética ha de estar en la base de las propuestas y soluciones, si bien éstas habrán de articularse a través del Derecho. Ahora bien, antes de poner palos en las ruedas de la innovación y el avance, antes de, en palabras de Tene y Polonetsky (2013, 2), vilipendiar el big data e imponer una regulación de mano dura, cabe establecer directrices y regulaciones legales y técnicas para limitar usos poco éticos, contrarios a derechos fundamentales y principios, en especial vinculados con la no discriminación y la privacidad, así como fortalecer el control y garantías del individuo.

De igual modo, a partir de la nacionalidad y ubicación de los mayores generadores de datos masivos, cabe discutir las ventajas e inconvenientes de modelos de autorregulación o heterorregulación, incluso modelos de regulación borrosa o nebulosa como se dan en ámbitos próximos como el de la nube (Cotino, 2015). Cabe preguntarse en razón de los derechos e intereses en juego y la naturaleza de la relación jurídica, cuál sería la tipología de fuentes apropiada, autorregulación, heterorregulación, códigos, normas de conducta, etc. La eficacia real de las decisiones que se adopten se hace depender de este tipo de elecciones, al igual que el papel del Derecho nacional y Derecho supranacional e internacional ante un fenómeno trasnacional. E incluso, sobre la base de existencia de normas, hay abordar jurídicamente el tratamiento trasnacional, ley aplicable y jurisdicción, así como negociabilidad del foro de cara a otras empresas con quienes contraten y respecto de los usuarios que generan los datos masivos. De igual modo, debe tenerse incluso en cuenta el potencial del futuro papel del big data y la AI para la misma generación y creación de normas ("algorithmic regulation") (Coglianese y Lehr, 2017; Alarie, Niblett y Yoon, 2016).

Para ello, una de las premisas jurídicas es determinar y en su caso diferenciar el tratamiento jurídico de la actividad de big data cuando se realiza ya por poderes públicos, ya por el sector privado. El marco jurídico puede ser diferente a partir de responsabilidad del estado, principio de legalidad, interés público, frente a la libertad de empresa y derechos en juego por el sector empresarial. Ya se trate del sector público o privado que realice acciones de big data, hay que plantearse la discrecionalidad o potestad para usar y tratar los datos masivos, la protección jurídica que tienen respecto de los métodos, tecnologías y resultados del big data, en

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

especial, debe tenerse en cuenta la propiedad industrial así como la concurrencia de posibles obligaciones de transparencia y puesta a disposición de los datos abiertos para su reutilización.

Sin perjuicio de la necesidad de sólidos presupuestos éticos, jurídicamente punto de partida deben ser los principios comunes del Derecho constitucional y en particular los derechos y libertades de las sociedades democráticas. Ellos no sólo quedan afectados por el big data y la inteligencia artificial, sino que son principios básicos que han de orientar las respuestas futuras. Ahora bien, puede ser necesaria una readecuación de tales principios (Sánchez Barrilao 2016). Incluso hay que plantearse el reconocimiento de nuevos derechos, como podría ser un derecho a la criptografía. Se trataría de una actualización o nueva versión que posibilite la *privacy* como derecho a que le dejen a uno sólo ("right to be let alone", Warren y Brandeis, parr. 1, 1890) o al más castizo derecho a que le "dejen a uno en paz".

Pero también es necesario un nuevo enfoque jurídico y dogmático en el tratamiento de los derechos fundamentales. El daño individual producido por el big data y la Inteligencia artificial puede ser imperceptible para el derecho fundamental desde la perspectiva del individuo titular del derecho, pero bien puede afectar masivamente a los derechos fundamentales de sectores o conjuntos de la sociedad de una manera relevante en esta dimensión colectiva. Dogmáticamente considero que puede ser necesario trabajar con una dimensión colectiva de los derechos que no es la habitual. De igual modo, no hay que eludir la potencialidad jurídica de los elementos y premisas de los derechos fundamentales concretos, como son la dignidad el libre desarrollo de la personalidad (art. 10. 1 CE). Pues bien, cabe acudir a estos elementos esenciales para afrontar algunos retos jurídicos.

La doctrina no ha subrayado esta cuestión respecto del big data, sólo en alguna medida respecto de la privacidad (De Tullio, 2016). Sin embargo, con una percepción práctica, el Parlamento Europeo acaba de subrayar la necesidad de garantizar efectivamente e incluso judicialmente a través de diversos derechos fundamentales el uso del big data, siempre que repercuta de manera relevante en las personas (Parlamento Europeo, Consideración 5).

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 131-150

3.1. Datos masivos, discriminaciones y brecha masivas

Cabe tener precaución por cuanto el big data crea nuevas brechas digitales. Tene y Polonetsky (2013, 4; siguen Manovich 2011) cuando describe de tres clases de personas en el ámbito de Big Data: los que generan los datos (consciente o inconscientemente), los que tienen los medios para recoger los datos, y aquellos que tienen experiencia para analizarlos. Y obviamente estos últimos son los privilegiados de este nuevo mundo. Son quienes fijarán las reglas reales de cómo se utilizarán y quiénes accederán al conocimiento. Quienes "pueden leer los datos", esto es, quienes tienen el conocimiento y medios para realizar el tratamiento masivo de datos pueden imponer barreras de acceso o limitar efectivamente o selectivamente el acceso a los datos o al conocimiento generado. Además, quienes no pueden acceder, los excluidos, no pueden evaluar la calidad y valor de los datos masivos y los análisis. Se crean así nuevas jerarquías políticas, económicas y sociales. Puede hablarse pues, de un big data rico y un pobre big data. Y ello no escapa al mundo universitario y de la investigación por cuanto que los que no tengan acceso a las cuotas, no podrán ni utilizar el conocimiento, pero tampoco evaluar la calidad metodológica de los productos del big data.

Por último, y –si se me permite- como nuevos *parias*, están quienes quedan en la periferia de los grandes datos pues ni los aportan. Como recuerda Lerman, millones de personas en todo el mundo permanecen en la periferia de las grandes datos. Así, sus preferencias y necesidades están en riesgo de ser ignoradas en las decisiones que se basen en el big data y la inteligencia artificial (Lerman 2013).

El big data y los algoritmos pueden heredar o reflejar perjuicios y patrones de exclusión o ser resultado de quienes han tomado decisiones anteriores (Barocas y Selbst 2016, 675, 714). Más allá de la intencionalidad –que es muy posible que no se dé en muchas ocasiones, se trata de un peligro objetivo que hay que prevenir.

Frente a estas situaciones es necesario redescubrir nuevas proyecciones de la igualdad y el derecho a la no discriminación, pues las dificultades para actuar, vigilar, controlar y corregirlas son complejas. Selbst apunta para Estados Unidos la necesidad de introducir técnicas como "discrimination impact assessments" siguiendo el modelo de declaraciones de impacto ambiental (Selbst, 2017, 50). Edwards llega a afirmar

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

la necesidad de una ética en el diseño incluso de una nueva "evaluación del impacto social" (Edwards, McAuley y Diver, 2016, 30).

Precisamente estas técnicas preventivas son bien conocidas en la UE. Así, tanto en el ámbito de la discriminación, con numerosas Directivas y legislación interna (Ley 4/2005, de 18 de febrero). Y especialmente son relevantes estos mecanismos en el ámbito de las nuevas tecnologías, los *Privacy Impact Assessment* (PIA). El nuevo Reglamento europeo de protección de datos apuesta por mecanismos proactivos y preventivos en vez de reactivos, que precisamente tienen especial importancia para el big data (ENISA, 2015). Así, el Reglamento impone la protección de datos desde el diseño y por defecto (art. 25), de modo que la privacidad se integre desde el inicio en la gestión y ciclo de vida del tratamiento de datos. Y lo mismo debe postularse respecto de la no discriminación, hay que integrar la no discriminación con estas medidas preventivas así como y especialmente en los casos en los que el Reglamento europeo exige antes de un tratamiento que los especialistas lleven a cabo una Evaluación de impacto de protección de datos (artículo 35 Reglamento). Y, precisamente, los usos del big data son claros candidatos a que dicha evaluación de impacto sea obligatoria, por cuanto suelen suponer la elaboración de perfiles y porque sobre el resultado del tratamiento se basan decisiones que produce efectos jurídicos sobre el individuo, o que pueden afectar de manera significativa a los individuos (art. 35. 3º Reglamento, AEPD- ISMS, 21, 2017). Hay que apostar, pues, en ir más allá de la protección de datos e integrar en estas medidas preventivas para evitar la discriminación.

Y entiendo que este tipo de garantías frente a la discriminación van a tener que combinarse con el reconocimiento de fuertes facultades de acceso y conocimiento de los algoritmos y los grandes datos que se manejan por parte de sectores especializados, tanto públicos como de la sociedad civil (reguladores, académicos industria, asociaciones de consumidores, etc. (FCC, 2014, 51). Y dicha transparencia ha de venir acompañada asimismo con el reconocimiento de fuertes potestades de control a autoridades independientes respecto de los *data brokers* que son claves en el sector. Sin perjuicio del control social por la sociedad civil especializada, entiendo que son idóneas las autoridades independientes cercanas al sector de las nuevas tecnologías, como lo son las autoridades de protección de datos (y transparencia en EU, AEPD-ISMS, 2017,26 y ss.).

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

El Parlamento Europeo ha alertado del peligro de "discriminación y el sesgo algorítmicos" (2017, consideración 20). Frente a ello, además de un "marco ético común sólido" o de "máxima prudencia" (cons. 20 y 31), hace referencia a la necesidad de "evaluaciones periódicas sobre la representatividad de los conjuntos de datos [y de] examinar la exactitud e importancia de las predicciones" (cons. 20).

3.2. De la personalización masiva de la información al fin de la esfera pública y la postverdad. Libertad de expresión artificial

La tendencia general a la personalización de servicios se da, singularmente, respecto del acceso a los contenidos de los medios de comunicación a través de Internet. Desde 2000 se discute si Internet en general y los servicios de personalización masiva y filtrado selectivo de contenidos, en particular, son positivos o no para la esfera pública y para la democracia deliberativa habermasiana, a lo que he dedicado mi atención (Cotino, 2013). Del lado más pesimista, siendo quizá el enfoque mayoritario, Turow y especialmente Susnstein sostienen que la personalización de contenidos conlleva una limitación del mercado de las ideas que es tan importante en una sociedad libre. Se considera que la personalización refuerza las posiciones particulares, sin apertura ni compromiso con lo diferente. Es más, se sostiene que la particularización de contenidos conlleva la desaparición del foro público. En la red y con los sistemas de personalización se crean "enclaves deliberativos" que no hacen sino que reforzar las posiciones individuales, contribuyendo a extremar y polarizar la esfera pública (Sunstein, 2001, 67 y 71). Por el contrario y del lado más optimista, Blumler y Gurevitch, Gimmler o Kellner consideran que Internet amplía la esfera pública, que propicia que los usuarios se encuentren y se relacionen con una gran diversidad de información y opinión diferente a la que habitualmente encontramos en la vida *off line*. Se indica en esta dirección que Internet propicia el hallazgo fortuito de ideas e información diferentes a través de sus enlaces.

Resulta extremadamente difícil mensurar objetivamente los efectos de la realidad de la selección y personalización de contenidos. De lo que no cabe duda es que el big data permite construir individualizada y masivamente las realidades que nos circundan. Así las cosas, algunas cuestiones jurídicas que plantea el big data y la inteligencia artificial están relacionadas con la "postverdad" y el Parlamento Europeo (2017, Cons. 13 y 14) también ha mostrado su preocupación. El riesgo de

ISSN 1989-7022

DILEMATA, *año 9 (2017), nº 24, 131-150*

manipulación de las personas en razón del uso del big data y la generación y empleo de patrones puede ser importante. Téngase en cuenta que se puede manipular el mundo virtual que nos rodea, conformar una realidad objetiva y subjetiva para el sujeto en razón de los procesos de personalización masiva de la información que hoy se permiten con las redes sociales y el big data. Y es que, por ejemplo, Solove (2014) demostró cómo se puede manipular el estado de ánimo de las personas a través de la personalización masiva de noticias e ingeniería semántica, transmitiendo noticias más o menos positivas, etc.

Ello suscita cuestiones del todo interés desde parámetros de libertad y libre desarrollo de la personalidad. En este sentido, Martín (2013) hace referencia a la inducción de comportamientos a través del uso de datos masivos. Al fin y al cabo, con el big data se puede inducir a un comportamiento, a quien votar, que estudiar, dónde viajar, dónde vivir, qué comprar. Es más, se puede inclinar más claramente hacia la ilegalidad, hacia la xenofobia, odio, discriminación, etc. Como recuerda este autor, hay una frontera muy fina entre influir en las decisiones a través de argumentos o información que permite valorar y tomar una decisión libremente, sobre la base de un juicio de valor formado por estímulos externos, y generar o inducir tales decisiones. En este último caso, el elemento de libertad en la toma de una decisión puede estar viciado por el uso de técnicas poco transparentes, que inducen al individuo a adoptar un determinado comportamiento o una determinada decisión, de manera inconsciente.

Así las cosas, resulta de interés preguntarse si los contenidos automatizados generados por máquinas están protegidos por la libertad de expresión (Wu, 2012). Y cabe en principio dar una respuesta afirmativa desde la perspectiva de las finalidades y funcionalidades del libre flujo de información en democracia (Massaro, Norton y Kaminski 2016 y 2017), si bien ello precisa de no pocas matizaciones para el futuro. También son muy relevantes las cuestiones que se suscitan por la responsabilidad ante los contenidos automatizados (Cheung*,* 2015*).* Igualmente hay que examinar con atención el uso de algoritmos de censura automatizada y la dificultad misma en su investigación (Narayanan y Zevenbergen, 2015).

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

4. De la "oscuridad en el diseño" a la "transparencia algorítmica" y su fundamentación en diversos derechos

Hartzog y Stutzman y hacen referencia a "la oscuridad por diseño" ("obscurity by design", 2013, 386, 452 y ss.) que es propia al big data. Como se ha adelantado, la falta de transparencia resulta uno de los problemas claves para afrontar los usos del big data y la inteligencia artificial. Frente a ello ahora se aboga por la "responsabilidad" y la transparencia algorítmicas (Parlamento Europeo, 2017, cons. N); cons. general. 1 y 21).

Resulta casi un privilegio acceder a los algoritmos, datos y el conocimiento generado, que incluso quedan fuera del acceso de los poderes públicos pese a la transcendencia pública de su uso público y privado. Es más, los poderes públicos no siempre acceden incluso en los casos en los que ellos mismos utilizan el big data y la IA en sus funciones públicas administrativas, policiales o judiciales. Han pasado de crear y controlar los instrumentos de acción a ser consumidores de los que les ofrece el sector privado (Joh, 2017). Los mismos científicos y académicos quedan en riesgo de exclusión e incluso para acceder al conocimiento se ven obligados a colaborar con el sector privado (Pasquale, 2015). Hay que dar una respuesta jurídica y fundamentar cómo y en qué medida se puede acceder a tal información, algoritmos y conocimientos generados.

En la tradición jurídica angloamericana el debido proceso (*due process*) puede fundamentar la necesaria transparencia y acceso a la información respecto de toda decisión basada en big data y IA que afecte a los derechos de las personas (Boyd 2011; Balkin, 2017) y cabe destacar el esfuerzo de Crawford y Schultz (2014) para vincular un derecho fundamental a las importantes implicaciones del big data. Y precisamente hacen el esfuerzo al partir de que la privacidad y datos personales quedan en buena medida superados. Pues bien, la idea básica es que en la tradición jurídica angloamericana, el debido proceso procesal prohíbe al gobierno privar a los derechos de un individuo a la vida, libertad o propiedad sin dar su acceso a información sobre la ciertos componentes básicos de procedimiento del proceso de adjudicación, así como los derechos para revisar y disputar la prueba en cuestión. La idea parte de que el uso del Big data en la toma de importantes decisiones debe nutrirse de garantías. Así, sería desarrollar el alcance del debido proceso para los sistemas informáticos de la administración pública, de modo que cualquier personal

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

evaluada o determinada en decisiones que le afecten por los datos masivos, tuviera ocasión de acceder a la información al respecto. Se trataría de derechos similares de quienes son juzgados por los tribunales.

En el ámbito europeo posiblemente el derecho de acceso y garantías de la justicia (art. 24 CE) no lleguen tan lejos y el acceso a la información parece venir más de la mano del derecho de acceso que forma parte del derecho a la protección de datos (art. 12 Reglamento europeo protección de datos).

En todo caso, y más allá de este derecho de acceso, cabe estar con Martín cuando propone el reconocimiento de un "derecho de acceso amplificado" (Martín, 2013), no limitado exclusivamente a los datos de que dispone un responsable de tratamiento, ni siquiera a los que les ha comunicado, sino sobre qué tratamientos concretos ha aplicado a los datos, qué información calculada se ha obtenido a partir de los datos y cuáles han sido los usos concretos, incluso respecto de las operaciones de disociación de la información. De esta manera, se daría respuesta tanto a los poderes derivados del autodeterminación informativa, como un mecanismo preventivo ante posibles tratamientos opacos de los datos personales.

5. Big data e inteligencia artificial en la aplicación de la ley y la justicia

De especial importancia resultan las posibilidades del big data y la IA en justicia, Administración y policía (Parlamento Europeo, 2017, cons. 25-32). Considero que hay que recibir favorablemente el uso del big data y la IA en las decisiones administrativas, policiales y judiciales. Frente a autores más negativos (Trazegnies 2013), considero que la decisión automatizada puede ser muy positiva si es revisada o completada con la intuición y el conocimiento experto humanos.

Ahora bien, la relevancia de estas decisiones a partir de big data y la IA para los derechos de los individuos y la propia importancia social de la cuestión llevan necesariamente a una especial sensibilidad en la materia, una "máxima prudencia" (Parlamento Europeo, 2017, cons. 31). Aquí, sin duda, las respuestas y garantías constitucionales vienen determinadas por las garantías del acceso a la justicia, la tutela judicial y el debido proceso (art. 24 CE), así como la prohibición de discriminaciones (art. 14 CE), especialmente peligrosas en el ámbito judicial o policial.

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 131-150

Y cabe cuestionarse especialmente la legitimidad del uso de sensores y monitoreo de impulsos y respuestas corporales de sospechosos en interrogatorios y el uso de IA respecto de los mismos (*human-computer interaction,* Thomasen, 2016).

También es de interés la potencialidad del big data y la IA en los mecanismos de resolución de conflictos ODR (Online Dispute Resolutions) es clara (De Mata, 2016). Incluso deben tenerse en cuenta las posibilidades de la justicia colaborativa que se concrete a partir de miles de interactuaciones de expertos como propuestas de resolución (Public-Centred Civil Justice Redesign, en Canadá (Salter y Thompson, 2017).

Stevenson y Wagoner (2014) se centran en la negociación y acuerdos en los procesos teniendo en cuenta la previsión del resultado en el juicio y los costos asociados. Tradicionalmente se han tenido en cuenta factores como los precedentes, la intuición y las interacciones con el juez, costes, etc. Sin embargo, cabe prever tendencias hacia el uso del big data para la toma de decisión de acuerdos y transacciones.

En EEUU, Joh (2014 y 2016) ha centrado acertadamente su atención en el uso policial de los grandes datos, la generación de zonas geográficas de riesgo, toma de decisiones de seguridad y otros patrones de predictibilidad.

6. Privacidad y la protección de datos y las dificultades de su garantía en el ámbito del big data

Sin perjuicio los derechos fundamentales mencionados, , hay a modo de una "vis atractiva" a abordar jurídicamente el big data desde la privacidad y, en concreto, el derecho de protección de datos personales. Más allá de la propia exigencia jurídica, se ha afirmado que el respeto de la privacidad ante el big data es una obligación moral de la sociedad (Allen, 2016). Krotoszynski (2015) también subraya que el respeto de la privacidad ante el big data es una premisa esencial para que sea posible cualquier deliberación democrática y del ejercicio mismo de la libertad de expresión vinculada a ella.

Como es sabido, el derecho de protección de datos confiere un "poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado", "atribuye a su

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos […] : el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos." (por todas, sentencia Tribunal Constitucional español 292/2000, FJ 7º).

El derecho de protección de datos personales ha girado estructuralmente hasta la fecha en el consentimiento del titular de los datos personales. No obstante, por diversos motivos esta columna vertebral de la protección de datos quebró hace tiempo. Rubinstein (2013, 1) afirma que la gran ola del big data "arrollará" (*overwhelm*) los clásicos principios y consentimiento del derecho de protección de datos personales. La sociedad no está dispuesta a renunciar al uso de las IT y no tiene una fuerte cultura de la privacidad, lo que lleva a hacer casi irreal o inefectiva la garantía del consentimiento (Oliver y Muñoz, 2014; Martínez 2014; Rubinstein 2013; Heeger, 2015). El consentimiento en la práctica viene masivamente por defecto. No es realista en modo alguno creer que existe un efectivo control de la información personal a través del consentimiento y los derechos que lo complementan. El consentimiento se torna en una *carta blanca* al descontrol del flujo de los datos personales. El consentimiento acaba configurándose como un simbolismo que conlleva, a la postre, al fracaso de la privacidad pretendida y a la inoperancia del sistema de protección.

Para más inri, el consentimiento se hace casi inservible e inoperante por la mayor complejidad del contexto tecnológico, la web 3. 0 y el big data (Oliver y Muñoz, 2014). Con relación a la información obligatoria para requerir el consentimiento, cabe cuestionarse el grado de detalle posible al respecto de la misma en razón de la especial naturaleza y desarrollo del big data, que hace bien difícil determinar las finalidades o comunicaciones que van a producirse. Y es que con los sistemas de inteligencia artificial y decisiones automatizadas es muy difícil consentir respecto de unas finalidades de uso de los datos que por lo general ni se conocen, ni se sospechan; ni se puede consentir respecto de unos algoritmos que se utilizarán, también desconocidos. Como apunta Martínez (2014), es una falacia afirmar que se pueda obtener el consentimiento para tratar una infinita cantidad de datos, por lo que llega a afirmar que hay que "arrinconar" el consentimiento a un ámbito "residual".

ISSN 1989-7022
DILEMATA, año 9 (2017), nº 24, 131-150

En la misma dirección, con los sistemas repartidos y el troceamiento de la información que son propios del *big data*, no es posible conocer la ubicación de los datos, ni tratamiento efectivo de los mismos. Por ello, también es muy difícil lograr un control de los datos personales por el usuario.

Pues bien, frente a las garantías subjetivas, que en buena medida dependen del consentimiento y la acción del individuo, deben reforzarse las obligaciones legales preventivas de privacidad en el diseño y por defecto y de la evaluación de impacto de protección de datos. Todo ello en la línea del reciente Reglamento de protección de datos de la UE garantías que ya han sido mencionadas al abordar la no discriminación (arts. 25 o 34 y ss. Reglamento, ENISA 2015, AEPD-ISMS 2017).

Otra de las claves jurídicas es que hay que centrar especialmente la atención en si se da la premisa de el big data implique un tratamiento de datos personales, puesto que de lo contrario, no procede aplicar el régimen jurídico de este derecho. Y es que si los macrodatos no son datos de personas concretas identificadas o identificables, no se aplica la legislación de protección de datos. Pues bien, una vía para escapar a la aplicación del exigente régimen de protección de datos es la anonimización, esto es, desvincular la información de su titular, por lo que deja de ser dato personal. La anonimización del big data presenta especiales problemas técnicos y jurídicos, s muy difícil hoy día garantizar que los datos no vuelvan a ser personales (AEPD-ISMS, 2017, pp. 40 y ss; Stalla-Bourdillon y Knight, 2017). A este respecto hay que seguir especialmente el Dictamen 5/2014, de 10 de abril, del Grupo de Trabajo del artículo 29 sobre anonimización. Asimismo, el Parlamento Europeo advierte de que pese a que se anonimicen los datos, otros derechos pueden quedar afectados (Parlamento Europeo, 2017, Cons. General 5, 7).

Cuando sí que sea aplicable el régimen de datos personales, es necesario fijar en qué términos pueden predicarse sus elementos básicos de consentimiento informado, principios de calidad, veracidad, finalidad, actualización, pertinencia, los derechos ARCO (acceso, rectificación, cancelación u oposición), el derecho a no ser sometidos a evaluaciones automatizadas de la persona, así como el tan famoso derecho al olvido. Estos derechos pueden jugar papeles muy complejos en el ámbito del big data.

No siempre es fácil aplicar el régimen de protección de datos al ámbito del big data y los algoritmos. Al respecto, que excede con mucho esta aproximación, cabe remitir

a muy recientes estudios a este respecto, especialmente el realizado por la AEPD-ISMS (2017).

Y, por último, como alertó la Comisión Federal de Comunicaciones de EEUU (FCC 2014, 55-56), los datos sensibles (raza, ideología, salud, orientación sexual, comisión de ilícitos, etc.) ya no son los que generarán los usos sensibles y problemáticos del big data. No en vano, con el big data es posible generar patrones y perfiles vinculables a estas categorías sensibles, como la raza, pero no a partir de datos ajenos en principio a estos datos sensibles (como por ejemplo, las pautas de fumar) y por tanto no contar con las especiales garantías de estos tratamientos.

Bibliografía

AEPD - ISMS Forum (eds.); Carlos Alberto Sáiz (coord.), (2017): *Código de buenas prácticas en protección de datos para proyectos de Big Data*, mayo, AEPD e ISMS Forum, Madrid.

Alarie, Benjamin; Niblett, Anthony y Yoon, Albert (2016): *Law in the Future*, mayo, https://ssrn.com/abstract=2787473

Allen, Anita L. (2016): "Protecting One's Own Privacy in a Big Data Economy" diciembre. *Harvard Law Review Forum,* Vol. 130, Pg. 71, 2016; *U of Penn Law School, Public Law Research Paper No. 17-1*. https://ssrn.com/abstract=2894545

Balkin, Jack M. (2017): "The Three Laws of Robotics in the Age of Big Data". *Ohio State Law Journal, Vol. 78, (2017), Forthcoming; Yale Law School, Public Law Research Paper No. 592.* https://ssrn.com/abstract=2890965

Barocas, Solon y Selbst, Andrew D. (2016): "Big Data's Disparate Impact". 104 *California Law Review 671* https://ssrn.com/abstract=2477899

Boyd Danah y Crawford Kate (2011): "Six Provocations for Big Data", *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, Acceso SSRN.

Burkholder, L, ed. (1992): *Philosophy and the Computer*, Boulder, San Francisco, and Oxford: Westview Press).

Coglianese, Cary and Lehr, David (2017): "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era", febrero, *Georgetown Law Journal, Forthcoming; U of Penn, Inst for Law & Econ Research Paper* No. 17-8. https://ssrn.com/abstract=2928293

Cotino Hueso, Lorenzo (2013): "La selección y personalización de noticias por el usuario de nuevas tecnologías", en Corredoira, Loreto y Cotino, Lorenzo (eds.) *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, pp. 41-56.

Cotino Hueso, Lorenzo (2015): "Algunas cuestiones clave de protección de datos en la nube. Hacia una 'regulación nebulosa'", en *Revista Catalana de Derecho Público* nº 51 (diciembre 2015), pp. 85-103 DOI: 10.2436/20.8030.01.55. http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-20.8030.01.55/n51-cotino-es.pdf

ISSN 1989-7022 DILEMATA, año 9 (2017), nº 24, 131-150

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

Crawford Kate y Schultz Jason (2014): "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", *Boston College Law Review, Vol. 55, No. 93, 2014, NYU School of Law, Public Law Research Paper No. 13-64, NYU Law and Economics Research Paper No. 13-36*. SSRN

De Tullio Maria Francesca (2016): "La privacy e i big data verso una dimensione costitizionale collettiva", *Politica del diritto*, Vol. 47, Nº. 4, págs. 637-696.

DemosEUROPA (2014): *Big and open data in Europe. A growth engine or a missed opportunity?,* estudio solicitado por la Comisión Europea al *Centre for European Strategy,* Sonia Buchholtz, Maciej Bukowski, Aleksander Śniegocki the Warsaw Institute for Economic Studies (WISE Institute) esponsorizado por Microsoft.http://www.bigopendata.eu/wp-content/uploads/2014/01/bod_europe_2020_full_report_singlepage.pdf

Edwards, Lilian; McAuley, Derek y Diver, Laurence (2016): "From Privacy Impact Assessment to Social Impact Assessment", Conference: 2016 IEEE Security and Privacy Workshops (SPW), pp. 53-57, doi:10.1109/SPW.2016.19

ENISA (2015): *Privacy by design in Big Data: An overview of privacy enhancing technologies in the era of Big Data analytics* (European Union Agency For Network And Information Security).

FCC (2014): *Data Brokers. A Call for Transparency and Accountability*, mayo.

Gartner, (2012): *Emerging Market Analysis: IT. Mexico, 2012 and beyond* Gartner.

Hartzog, Woodrow y Stutzman, Frederic D. (2013): "Obscurity by Design", junio *Washington Law Review,* Vol. 88, https://ssrn.com/abstract=2284583

Heeger, Eva (2015): "Controlling Your Online Profile: Reality or an Illusion? A Research into Informed Consent as a Mechanism to Regulate Commercial Profiling", agosto, http://dx.doi.org/10.2139/ssrn.2658651

Joh Elizabeth E. (2014): "Policing by Numbers: Big Data and the Fourth Amendment", en 89 *Wash. L. Rev*. 35.

Joh, Elizabeth E. (2016): "Policing Police Robots" (agosto). *64 UCLA L. Rev. Discourse 516* https://ssrn.com/abstract=2817185

Joh, Elizabeth E. (2017): "The Undue Influence of Surveillance Technology Companies on Policing", febrero, *N.Y.U. L. Review Online* (2017). https://ssrn.com/abstract=2924620

Krotoszynski Jr., Ronald J. (2015): "Reconciling Privacy and Speech in the Era of Big Data: A Comparative Legal Analysis", *William & Mary Law Review, Vol. 56, 1279, 2015; U of Alabama Legal Studies Research Paper,* https://ssrn.com/abstract=2605508

Latour, B. (2009):."Tarde's idea of quantification", in *The Social After Gabriel Tarde:* Debates and Assessments, (ed M. Candea), London: Routledge, pp. 145-162.

Lerman, Jonas (2013): "Big Data and Its Exclusions", en *Stanford Law Review Online, 66 Stanford Law Review Online* 55, SSRN.

Manovich, Lev (2012): "Trending: The Promises and the Challenges of Big Social Data", in *Debates in the digital humanities* (Matthew Gold, Editor, The University of Minnesota Press, 2012).

Martín Miralles, Ramón (2013): "Big Data vs Small low", *Congrés IDP 2013 Butlletí +Kdades: Butlletí electrònic de tecnologia, auditoria i seguretat de la informació*, Nº. 24, 2013, pp. 7-8, acceso en http://dialnet.unirioja.es/servlet/extart?codigo=4329765

Martínez, Ricard (2014): "Ética y privacidad de los datos", texto escrito de la *Jornada: Big Data: de la investigación científica a la gestión empresarial*, Fundación Ramón Areces, 3 de julio de 2014, acceso en http://sgfm.elcorteingles.es/SGFM/FRA/recursos/conferencias/ppt/1776180509_1472014102438.docx

Massaro, Toni M. and Norton, Helen L. y Kaminski, Margot E. (2016): "Siri-ously? Free Speech Rights and Artificial Intelligence" octubre, *110 Northwestern University Law Review 1169; Arizona Legal Studies Discussion Paper No. 15-29.* https://ssrn.com/abstract=2643043

Massaro, Toni M. and Norton, Helen L. y Kaminski, Margot E. (2017): "Siri-ously 2.0: What Artificial Intelligence Reveals about the First Amendment", enero. *Minnesota Law Review (Forthcoming); Arizona Legal Studies Discussion Paper No. 17-01; Ohio State Public Law Working Paper No. 374*. https://ssrn.com/abstract=2896174

Mayer-Schönberger, Viktor y Cukier, Kenneth (2013 a): *Big Data: A Revolution That Will Transform How We Live, Work, and Think;* ahora en *Big data. La revolución de los datos masivos*, Turner Publicaciones.

Mayer-Schönberger, Viktor y Cukier, Kenneth (2013 b): "The Dictatorship of Data", MIT Technology Review, mayo de 2013 https://www.technologyreview.com/s/514591/the-dictatorship-of-data/ acceso en español en https://www.technologyreview.es/s/3564/la-dictadura-de-los-datos (trad. Francisco Reyes).

Narayanan, Arvind y Zevenbergen, Bendert (2015): *No Encore for Encore? Ethical Questions for Web-Based Censorship Measurement*, septiembre, http://dx.doi.org/10.2139/ssrn.2665148

Nilsson Nils (1980): *Principles of artificial intelligence*, Palo Alto, California: Tioga Press.

O'Neil, C. (2016): *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown

Oliver A. Daniel y Muñoz José Félix (2014): "El mito del consentimiento, o por qué un sistema individualista de protección de datos (ya) no sirve para (casi) nada", en Valero Torrijos, Julián: *La protección de los datos personales en Internet ante la innovación tecnológica, Aranzadi*, Cizur Menor, 2014.

Parlamento Europeo (2017): *Resolución de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley* (2016/2225(INI)).

Pasquale, Frank A., (2015): "Privacy, Autonomy, and Internet Platforms", en *Privacy in the Modern Age: The Search for Solutions*, pp. 165-174 (Marc Rotenberg, Julia Horwitz, and Jeramie Scott eds., New Press 2015).; *U of Maryland Legal Studies Research Paper No. 2016-10.* https://ssrn.com/abstract=2737413

Puyol Moreno, Javier (2014): "Una aproximación a Big Data", en *Revista de Derecho* UNED, núm. 14, 2014, págs. 471-505. Acceso en Dialnet

Richards Neil M. y King Jonathan H. (2013): "Three Paradoxes of Big Data", en 66 Stanford Law Review Online 41.

Rubinstein Ira (2013): "Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, NYU School of Law, Public Law Research Paper No. 12-56. SSRN

Salter, Shannon and Thompson, Darin (2017): "Public-Centred Civil Justice Redesign: A Case Study of the British Columbia Civil Resolution Tribunal (abril). *McGill Journal of Dispute Resolution, Vol. 3, 2016-2017*. https://ssrn.com/abstract=2955796

Samuel Warren y Louis Brandeis (1890): "The Right to Privacy" (*4 Harvard L.R*. 193).

Sánchez Barrilao, Juan Francisco (2016): "El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional", *Estudios de Deusto: revista de la Universidad de Deusto*, Vol. 64, Nº. 2, págs. 225-258.

Selbst, Andrew D. (2017): *Disparate Impact in Big Data Policing*, *Georgia Law Review*, Forthcoming. https://ssrn.com/abstract=2819182

ISSN 1989-7022

DILEMATA, año 9 (2017), nº 24, 131-150

ISSN 1989-7022

SMART-Comisión Europea (2013): 2013/0063 - Study on a "European data market", encargado por la Comisión http://ec.europa.eu/digital-agenda/en/news/smart-20130063-study-european-data-market-and-related-services

Soares, Sunil (2012) *Big Data Governance: An Emerging Imperative*, MC Press, LLC.

Solove Daniel J. (2014): "Facebook's Psych Experiment: Consent, Privacy, and Manipulation, en *Debates and Assessments*, ed M. Candea, London: Routledge, pp. 145-162.

Stalla-Bourdillon, Sophie y Knight, Alison (2017): · Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data", marzo *Wisconsin International Law Journal*, https://ssrn.com/abstract=2927945

Stevenson Drury D. y Wagoner Nicholas J. "Bargaining in the Shadow of Big Data", en *Florida Law Review*, Vol. 66, No. 5, 2014

Sunstein, Cass R. (2001): *Republic.com*, Princeton University Press, luego en *República.com. Internet, democracia y libertad*, Paidós, Madrid, 2003.

Surden, Harry (2017): *Values Embedded in Legal Artificial Intelligence*, marzo, https://ssrn.com/abstract=2932333

Tene Omer y Polonetsky Jules (2013): "Judged by the Tin Man: Individual Rights in the Age of Big Data", en *Journal of Telecommunications and High Technology Law*, agosto 2013. SSRN

Thatcher, J. (2014): "Living on Fumes: Digital Footprints, Data Fumes, and the Limitations of Spatial Big Data". *International Journal of Communication*, *8*, 19. http://ijoc.org/index.php/ijoc/article/view/2174

Thomasen, Kristen (2016): "Examining the constitutionality of robot-enhanced interrogation", en yan Calo, A. Michael Froomkin & Ian Kerr, eds., (2016). *Robot Law*, Edward Elgar (ed.). pp. 306-333.

Trazegnies Granda, Fernando de (2013): "Seguirán existiendo jueces en el futuro?: el razonamiento judicial y la inteligencia artificial", *Ius Et Veritas*, nº. 47, pp. 112-131

Wu, Tim (2012): "Free Speech for Computers?", en The New York Times, 19 junio, http://www.nytimes.com/2012/06/20/opinion/free-speech-for-compute