TESI DOCTORAL UPF / 2019

Universitat Pompeu Fabra Barcelona

Big data, poder y libertad
Sobre el impacto social y político de la vigilancia masiva

Sara Suárez Gonzalo

BIG DATA, PODER Y LIBERTAD

Sobre el impacto social y político de la vigilancia masiva

Sara Suárez Gonzalo

DIRECTOR DE LA TESI: Dr. Frederic Guerrero Solé

TESI DOCTORAL UPF / 2019
DEPARTAMENT DE COMUNICACIÓ

Universitat Pompeu Fabra
Barcelona

Título: Big data poder y libertad. Sobre el impacto social y político de la vigilancia masiva.

Title: Big data, power and freedom. On the social and political impact of massive surveillance.

La reproducción y la distribución del contenido de los artículos publicados (o aceptados para publicación) que se incluyen en esta tesis por compendio deben respetar las exigencias de las revistas editoras.

Agradecimientos

Quiero dar las gracias a todas las personas que me han acompañado y me han ayudado durante, al menos, estos últimos cuatro años.

En primer lugar, gracias a las personas del Departamento de Comunicación de la Universitat Pompeu Fabra. Especialmente a mi director, Frederic Guerrero, con quien he compartido el entusiasmo y la inquietud por el tema de esta tesis, y a quien, sobre todo, le agradezco que haya confiado en mi trabajo. A Lluís Mas, por su apoyo, y por escribir con nosotros uno de los artículos que la componen. A Francesc Salgado, Jaume Guillamet, Lluís Codina, Rafa Pedraza, José Fernández, Carles Pont y al grupo de POLCOM, por las oportunidades. Y gracias a las amigas Jucinara, Lucía, Yosra y Cristina, y al amigo Lander, que han estado conmigo, más cerca o más lejos.

Por otra parte, quiero darle las gracias a Aurora García, que creyó en mi capacidad para la investigación y me guió en los primeros pasos, y a José Luís Martí, que en la parte final de esta tesis me ha ayudado a entender la teoría republicana.

I would also like to thank Tsjalling E. Swiestra for supporting my candidacy for the YERUN Research Mobility Award and for the kind welcome at the Department of Philosophy of Maastricht University. También a Rodrigo de Oliveira y al grupo STS-b de la Universitat Autònoma de Barcelona, por invitarme a su seminario.

Gracias a las personas con las que he vivido el día a día laboral, por todo lo que me han enseñado. A los compañeros del CCCB y de ESADE. A los equipazos de Alumni UPF y de Carreres Professionals. Especialmente a María Escrivá, Pep, Álvaro, Helena, Marc, Júlia y María Mayans. I gràcies a tota la bona gent del Consell de l'Audiovisual de Catalunya, i encara més a la Sandra, la Sylvia, el Martí, l'Esther, l'Imma, la Davínia, el Carles i el Salvador, que han patit amb mi l'etapa final i m'han donat tot el seu suport.

Por último, y sobre todo, gracias a mi gran compañero, Pablo Scotto, con quien he discutido cada aspecto de esta tesis. Gracias a mi familia, por su ayuda y su cariño y por hacer esto conmigo. A mi madre (que en el 92 me trajo hasta *aquí*), a mi padre, a Rodolfo, a Lucas, a Alejandro y a mi abuela, a sus 93. Gracias también a Juana, a Lucía, a Elena, a Andrea y a Diego. Y a las amigas, Anaïs, Marta, Raquel y Laura.

Resumen

Esta tesis doctoral reflexiona sobre el impacto social y político de la explotación de datos masivos a nivel europeo. Cumple dos objetivos principales. En primer lugar, define el contexto general en el que se produce esta explotación, a través del análisis de cinco factores: a) la lógica de generación, recopilación y procesamiento de los datos masivos; b) el modelo de negocio de las grandes corporaciones de servicios digitales; c) el discurso mediático dominante acerca de las tecnologías big data; d) las reacciones sociales y formas de resistencia ante este nuevo escenario; y e) el reglamento europeo de protección de datos personales, incluyendo su fundamentación conceptual. En segundo lugar, discute en qué medida estos cinco factores favorecen u obstaculizan la privacidad, la libertad y el control sobre los datos, desde una perspectiva fundamentada en la teoría crítica del capitalismo, la filosofía republicana, la teoría política feminista y la teoría del *framing*.

La investigación se compone de cinco publicaciones: 1. *La conversación sobre big data en Twitter. Una primera aproximación al análisis del discurso dominante.* 2. *Tay is you. The attribution of responsibility in the algorithmic culture.* 3. *Big social data: límites del modelo notice and choice para la protección de la privacidad.* 4. *Your likes, your vote? Big personal data exploitation and media manipulation in the US presidential election campaign of Donald Trump in 2016.* 5. *Personal data are political. A feminist view on privacy and personal data protection.* Esta memoria contextualiza, organiza y relaciona las aportaciones principales de estos artículos.

Abstract

This doctoral thesis reflects on the social and political impact of big data exploitation at the European level. The research fulfils two main objectives. Firstly, it defines the general context in which this exploitation is embedded, through the analysis of five factors: a) the logic of big data generation, gathering and processing; b) the business model of digital services corporations; c) the dominant media discourse on big data technologies; d) the social reactions and forms of resistance to this new scenario; and e) the European regulation on personal data protection, including its conceptual foundations. Secondly, it discusses to what extent these five factors favour or hinder privacy, freedom and control over data, from the lens of critical theory of capitalism, republican philosophy, feminist political theory and framing theory.

The study consists of five publications: 1. *La conversación sobre big data en Twitter. Una primera aproximación al análisis del discurso dominante*. 2. *Tay is you. The attribution of responsibility in the algorithmic culture*. 3. *Big social data: límites del modelo notice and choice para la protección de la privacidad*. 4. *Your likes, your vote? Big personal data exploitation and media manipulation in the US presidential election campaign of Donald Trump in 2016*. 5. *Personal data are political. A feminist view on privacy and personal data protection*. This report contextualizes, organizes and connects the main contributions of these papers.

Prólogo

> What makes the world portrayed in the book [*Ishiguro's Never Let Me Go*] truly horrifying, however, is something else: its protagonists do not perceive it as we do. The clones do not see their situation as unjust. They were created for, and socialized into, this highly exploitative order. Because it is the only society they know, its terms appear natural and normal to them. Granted, one of them, Tommy, is often angry. As a child living at Hailsham, he is prone to outbursts of temper for no apparent reason. But the others, including his closest friend Kathy, treat his rage as a personal problem. No one, including Tommy himself, ever considers the possibility that he has good reason to be angry. All encourage him in various ways to calm down; and so he does.
>
> […]
>
> Eventually, they do learn the truth. But by that point, they are not disposed to feel indignation. Responding with sorrow instead of anger, the adolescent clones find their situation unfortunate, but they do not judge it—or the basic structure that underlies it—to be unjust. Nor do they contemplate collective protest or revolution. On the contrary, they latch onto the promise of escape for a lucky few.
>
> On Justice (Fraser, 2012: 45, 47)

On Justice, de Nancy Fraser (2012) reflexiona sobre *Never Let Me Go*, una conocida novela del premio Nobel de literatura Kazuo Ishiguro (2005).

Sus protagonistas son Kathy, Tommy y Ruth, tres jóvenes clones humanos creados para abastecer un novedoso *programa de donaciones* en la Gran Bretaña de finales de los 90. La narración se sitúa en un momento en que esta forma de donación emergía como un avance científico y tecnológico imparable, sin tiempo para hacer balance, ni las preguntas pertinentes.

Hasta su adolescencia, los clones son criados en Hailsham, un apacible aunque escondido *internado* para alumnos *especiales* como ellos, regentado por un grupo de *guardianes* que se enorgullecen de *protegerlos* y de *educarlos*. Crecen en un régimen extrañamente estricto en lo saludable, lo artístico y lo social, ignorando la crudeza de su condición, aunque sin ser completamente ajenos a ella. Durante años, los guardianes les van desvelando esta realidad en pequeñas dosis, que los clones normalizan, sin rebelarse contra ella, ni alterar el proceso: al alcanzar la edad adulta se convertirán en *donantes* e irán cediendo sus órganos a los *originales* hasta *consumar*. Con el tiempo, Ruth y Tommy, enamorados, acaban obsesionándose con la posibilidad de que Madame, un personaje misterioso que les visitaba en Hailsham para llevarse a *la Galería* las

producciones artísticas que mejor reflejasen su *alma*, se apiade de ellos y les conceda un *aplazamiento*.

El sentido y la intención de la novela han sido muy discutidos. Algunos ven en ella una reivindicación de las cosas verdaderamente importantes de la vida. Otros, una distopía sobre el futuro de la biotecnología. Ishiguro la ha calificado siempre como una historia sobre el amor y la amistad frente a la evidencia de la muerte. En un acto público celebrado en 2010, al ser preguntado sobre por qué los protagonistas no escapan de su dramática situación, aseguró haberla escrito profundamente atraído por la forma en que las personas aceptan ciertas certezas que les vienen dadas como irremediables, sin enfrentarlas ni hacer lo posible por escapar de ellas: "I'm fascinated by the extent to which people don't run away, and I think if you look around us, that is the remarkable fact", dijo. "Sometimes is just passivity, sometimes is simply about perspective. We don't have the perspective to think about running away."

La interpretación que hace Fraser de *Never Let Me Go* va más allá de las explicaciones puramente individuales o psicológicas a las reacciones de Kathy, Tommy y Ruth. Identifica, en cambio, las causas de sus injustas "circunstancias personales" y de la aparente pasividad con la que las asumen, en el orden social representado en el libro. Si esas circunstancias son injustas es porque la estructura básica en la que se inscriben es, objetivamente, explotadora: sus vidas y sus decisiones están subordinadas a los intereses de otros.

Fraser encuentra en la novela los elementos distintivos de una forma de opresión *sutil*, que no es violenta ni repentina y que, precisamente por eso, es extremadamente eficaz. Los clones no son obligados a formar parte de ese sistema de cooperación, no son deliberadamente manipulados, ni engañados. Más bien, es una injusticia que ellos mismos naturalizan de forma paulatina y sosegada, como en la anécdota de la rana y el agua hirviendo: "The Hailsham policy of titrating knowledge keeps the child-clones in the pot" (Fraser, 2012: 47). Lo más grave, es que esta injusticia se esconde tras una apariencia amable y benevolente que, sin embargo, limita la capacidad de los clones para entender su realidad como injusta y tomar el control para enfrentarla, revertirla o escapar de ella. Esta situación se prolonga durante su edad adulta, cuando Hailsham y las Cottages —el centro en el que viven, ya sin guardianes, mientras son adolescentes—

han quedado atrás. Ahora nadie les indica lo que tienen que hacer y se mueven "libremente" por el país en sus coches particulares, aunque de centro en centro de *donación*. Es una injusticia que no da lugar a una rebelión individual, ni colectiva, sino que conduce, con el tiempo, a la frustración, a la aceptación de un infortunio que se mezcla y se confunde con las idas y venidas de la trayectoria personal.

Never Let Me Go dibuja un entorno en el cual las explicaciones estructurales a las desigualdades sociales son marginalizadas y los esquemas interpretativos y discursivos dominantes responden a los intereses de la explotación. Las personas son inducidas a buscar soluciones personales a los problemas de sus *preciadas* e *irremplazables* vidas. "Convinced that their inferior status is deserved," dice Fraser (2012: 46), "they bury their legitimate anger and tie themselves in emotional knots."

Si el texto de Fraser es interesante para introducir el sentido y la intención de esta tesis doctoral es porque, partiendo del relato de Ishiguro, se pregunta por el lugar de la justicia en las sociedades de consumo masivo y reflexiona sobre las dificultades para identificarla y alcanzarla, en un momento en que el individualismo es imperante. *On Justice* alienta a pensar en la justicia a través de la negación de la injusticia experimentada. Reivindica la importancia de cuestionar la tendencia a redefinir las desigualdades estructurales como problemas personales y llama a desconfiar de aquellas sociedades que idealizan la libertad, el amor, el mundo interior y la vida privada, pero sistemáticamente obstaculizan el acceso a las condiciones materiales e inmateriales necesarias para su realización.

El mismo título de la novela, *Never Let Me Go* ("nunca me dejes ir", oficialmente traducido al castellano como *Nunca me abandones*), tiene una significación especial. No es una reivindicación, ni una queja, ni una llamada a la acción. Es una súplica, un ruego. Una apelación a la bondad de un poder distante, a quien Ruth y Tommy buscan contentar hasta el final, confiándole sus destinos.

No es solamente una historia sobre la docilidad o la resignación. Es, ante todo, una historia de dominación sin interferencia, ligada a la falta de reflexión que a menudo acompaña al avance tecnológico y a las paradojas de un individualismo que corrompe el

valor intrínseco de la individualidad, al disociarla de la estructura social en la que se desarrolla.

* * *

En 2013, Edward Snowden filtró, a través de los diarios *The Guardian* y *The Washington Post*, numerosos documentos que destaparon varios programas de vigilancia masiva encabezados por la Agencia de Seguridad Nacional estadounidense (NSA, por sus siglas en inglés), y de los que también se habría beneficiado el Cuartel General de Comunicaciones del Gobierno británico (Gellman, y Poitras, 7 de junio de 2013; Greenwald, MacAskill y Poitras, 11 de junio de 2013; MacAskill, 10 de junio de 2013).

Uno de esos programas era PRISM, surgido de las cenizas de otro anterior, creado en 2007. De hecho, no era la primera vez que los servicios de inteligencia estadounidenses colaboraban con empresas que les ayudaban a interceptar el tráfico de datos o a acceder a información que les estaba restringida. La novedad de PRISM fue que la NSA obtenía la información directamente de los servidores de gigantes digitales como Google, Facebook, Microsoft o Apple. Estas revelaciones crearon un clima de alerta pública sobre los riesgos de la vigilancia "estatal". Sin embargo, vale la pena recordar que, por comprometida que fuese la información a la que pudo acceder la NSA, esta ya estaba contenida en los servidores de dichas grandes empresas, sin cuya colaboración el caso no hubiera sido posible.

El mismo año 2013, "big data" fue tendencia tecnológica a escala mundial, Mayer-Schönberger y Cukier (2013) publicaron su influyente libro *Big Data: A Revolution That Will Transform How We Live, Work and Think* y el análisis de datos masivos empezó a sonar con fuerza como el nuevo paradigma de la comunicación masiva personalizada. Yo preparaba mi Trabajo Final de Grado y, sin ser consciente de la importancia que el tema adquiriría en los años siguientes, empecé a preguntarme cuáles eran las características del fenómeno y cómo afectaría a la vida de las personas. Esta tesis doctoral tiene su origen entonces.

Lo que me preocupaba en aquel momento de las tecnologías big data, y lo que me preocupa ahora, no es tanto que alguien esté espiando a las personas, obteniendo los

datos sin "su permiso", ni que usando esos datos se les pueda obligar a actuar de un modo distinto al que ellas hubieran deseado. Estos riesgos existen y hay casos que así lo acreditan. Sin embargo, este no es el punto de partida de esta tesis, ni su foco de atención principal. No me preocupan única, ni particularmente, los casos de datos "robados" o utilizados ilícitamente, sino también aquellos en los que estos se obtienen de una forma legal y consentida por las personas.

Mi preocupación se intensificó al conocer varios estudios que demuestran que, ante el auge de las tecnologías big data, las personas están cada vez más preocupadas por su privacidad, pero no actúan en consecuencia. Esto, que habitualmente se conoce como la *paradoja de la privacidad* (Barnes, 2006), suele explicarse atendiendo a las características personales de los individuos.

Durante un breve periodo de tiempo, que coincidió con mis estudios de Máster, pensé en dedicar parte de mi investigación a analizar esta cuestión desde una perspectiva empírica, centrada en lo *personal*. En principio, parece lógico: si una persona dice estar *preocupada* por su privacidad, pero no *deja de usar* servicios por los que le piden sus datos, será que, en el fondo, no lo está tanto. O que ha valorado su situación y *prefiere* ceder sus datos a preservar su privacidad. O que *comprende* su privacidad de una forma particular, tal vez dependiendo de su edad, su género, su nivel de estudios…

A medida que he avanzado en mi investigación, la propia naturaleza del fenómeno estudiado, me ha llevado a un campo más teórico. Con el tiempo he entendido que el problema tiene que ver con el contexto de desigualdad en el que se insertan las tecnologías big data, y el cual ayudan a perpetuar. También con los términos que han acompañado a su introducción social, fomentados por los discursos (y la falta de discursos) corporativos, jurídicos, mediáticos y políticos. Se trata de un escenario que limita la capacidad de la ciudadanía para controlar la situación. Es una injusticia que explica, al igual que en el caso de Tommy y Ruth, la aparente paradoja.

Espero que, en un momento de auge tecnológico, en el que es difícil pararse y tomar distancia respecto a lo nuevo, esta investigación contribuya plantear algunas preguntas pertinentes y, a su vez, esté en grado de avanzar algunas respuestas.

Cómo leer esta tesis

Esta investigación, realizada entre los años 2015 y 2019, cumple las exigencias de cualquiera de las dos modalidades establecidas por la *Normativa para la presentación de Tesis por compendio de publicaciones* del Departamento de Comunicación de la Universitat Pompeu Fabra.

En concreto, se ha guiado por la Modalidad A, aprobada por la Comisión Académica de Doctorado el 12 de febrero de 2019. Esta establece que la tesis debe contener tres artículos publicados (o aceptados para su publicación) en revistas recogidas en alguno de los repertorios aceptados por las agencias de evaluación españolas. Preferentemente: CARHUS Plus+ 2014, ERIH PLUS, RESH, FECYT, MIAR, Web of Science y Scopus.

La normativa requiere también que, al menos, dos de los tres artículos hayan sido publicados (o aceptados para su publicación) en una revista indexada en Scopus o en la colección principal de Web of Science. Además, la doctoranda debe ser la primera firmante en todos los artículos y al menos uno de ellos debe haber sido publicado en inglés.

Por otra parte, la coherencia investigadora de los artículos del compendio debe ser razonada y argumentada en la "memoria" de la tesis. En esta memoria, se deben incorporar los datos referenciales completos de cada ítem que forme parte de la tesis y los textos de los mismos. En caso de que no sea posible aportar los textos completos, se deben adjuntar la carta o el correo electrónico de aceptación de la publicación correspondiente y documento original (o *pre-print*) completo.

En concreto, esta tesis la conforman la presente memoria y cinco artículos publicados en revistas de investigación científica indexadas en las bases de datos requeridas. La lista de los artículos y sus datos de indexación se aportan en la página 51.

Índice

Introducción

Durante la década de 1990 se registró una variedad y un volumen de datos sin precedentes que, además, se generaron a mayor velocidad que nunca antes (Laney, 2001). En 1997, Cox y Ellsworth, investigadores de la Administración Nacional estadounidense de la Aeronáutica y del Espacio (NASA, por sus siglas en inglés:), utilizaron el término "big data" (datos masivos) para designar a aquellos conjuntos de datos demasiado grandes como para poder ser procesados por la memoria principal, el disco local o cualquier otro disco remoto de los ordenadores del momento. El término, por tanto, surgió para denominar un problema de magnitud.

También en 1997, el científico de la computación Michael Lesk predijo que el desarrollo tecnológico permitiría disponer, en solo unos años, de espacio de almacenamiento suficiente para registrar en datos casi toda expresión de la actividad humana. Esto, alertó Lesk, supondría que los humanos no podrían procesar ni hacer "útil" tal cantidad de información, por lo que sería necesario evaluar automáticamente y de forma permanente la información para decidir, incluso, a qué partes de ella dedicar atención humana. Efectivamente, la cantidad de datos continuó en aumento de forma exponencial en los años siguientes y, de forma paralela, se desarrollaron las tecnologías necesarias para almacenar y analizar todos esos datos.

Así, el problema al que se referían Cox y Ellsworth fue rápidamente superado por el desarrollo tecnológico (Manovich, 2012) y, en consecuencia, el término "big data" perdió parte de su sentido inicial. En 2011, boyd y Crawford, ya hablaban de un nuevo "ecosistema de datos", que no solo se caracterizaba por la cantidad de datos, sino también por las conexiones que se podía trazar entre ellos al analizarlos en conjunto, sin importar en qué formato habían sido generados o de qué fuente procedían.

Las definiciones, entonces, pasaron de referirse únicamente al tamaño de las bases de datos, a describir cuestiones relacionadas con el *valor* y la *utilidad* de los datos y con las tecnologías de análisis de los mismos (Mayer-Schönberger y Cukier, 2013; Minelli, Chambers y Dhiraj, 2013; Kalyvas y Oberly, 2014). Pese a todo, la expresión "big data" se ha seguido utilizando para aludir tanto a cantidades de datos especialmente grandes, como a una nueva forma de generación, recopilación y análisis y a las técnicas que lo

hacen posible. Es decir, *big data* hace referencia a todo un fenómeno complejo. Por este motivo, son muchos los autores y las autoras —entre los cuales boyd y Crawford (2011), Manovich (2012) o Ward y Barker (2013)— que han acusado una cierta ambigüedad del término.[1]

El amplio abanico de posibilidades que abre el análisis de datos masivos ha atraído y atrae a cada vez más sectores interesados. Algunos ejemplos son la negociación de alta frecuencia de los mercados financieros (Karppi y Crawford, 2016), la mejora de los tratamientos médicos (Sarker *et al.*, 2015), la predicción y la gestión de desastres naturales y otras situaciones de crisis y emergencia (Castillo, 2016), o la persecución del crimen y el terrorismo (Bogomolov *et al.*, 2014). Pero, la personalización de mensajes, la recomendación de contenidos, o las predicciones de mercado son algunos de sus objetivos más frecuentes. Esto ha abierto un nuevo sector de mercado, cuyo poder se concentra en las grandes corporaciones tecnológicas proveedoras de servicios digitales, a menudo conocidas como GAFAM (Google, Apple, Facebook, Amazon y Microsoft) o AAFAM (Alphabet, Apple, Facebook, Amazon y Microsoft) (McChesney, 2013; Tufekci, 2017).

Al mismo tiempo, el fenómeno de los datos masivos ha despertado un gran interés en el mundo académico desde diferentes enfoques, tanto a nivel práctico como teórico. Entre otros, se han multiplicado los estudios que examinan, desde una perspectiva crítica e interdisciplinar, las oportunidades y los desafíos que plantean el fenómeno *big data* y las tecnológicas basadas en el procesamiento de datos en el plano social y político.

Contexto teórico

En términos generales, la presente tesis doctoral se enmarca en esta tendencia de estudios críticos sobre el fenómeno big data, que reúne a investigadoras e investigadores de áreas de conocimiento que van desde la Comunicación, la Ciencia de la Información, la Sociología, la Filosofía, la Teoría y la Economía Políticas, la Psicología, la

[1] En general, en esta tesis doctoral, "big data" se utiliza como sustantivo para referirse a las cantidades masivas de datos y al fenómeno por el cual estos han aumentado enormemente, y como adjetivo para hacer referencia a aquellos procesos específicos vinculados al tratamiento de los datos masivos. Fundamentalmente en los casos siguientes: tecnología big data, explotación big data, lógica big data, generación big data, recopilación big data, o procesamiento big data.

Biblioteconomía o el Derecho, a otras como la Computación, la Informática, la Ingeniería o la Matemática. Los estudios de esta tendencia se engloban bajo el nombre de estudios críticos en ciencia de datos, estudios sobre vigilancia o, de forma más amplia, estudios sobre ciencia, tecnología y sociedad (*STS* por sus siglas en inglés).

La mayoría de las investigadoras y de los investigadores más influyentes de esta tendencia desarrollan su trabajo vinculados a universidades estadounidenses. Algunos de ellos y de ellas son: danah boyd y Kate Crawford, investigadoras del Massachusetts Institute of Technology (MIT), autoras de, entre muchos otros, *Six Provocations for Big Data* (2011) y fundadoras de los centros de investigación Data & Society Research Institute y el AI Now Institute, respectivamente. Viktor Mayer-Schönberger, profesor e investigador de Gobernanza y Derecho de Internet en el Oxford Internet Institute y autor, junto a Kenneth Cukier de *Big Data: A Revolution That Will Transform How We Live, Work and Think* (2013). Frank Pasquale, profesor e investigador de Derecho y políticas de las tecnologías en la University of Maryland, cuya obra más destacada hasta el momento es *The Black Box Society: The Secret Algorithms That Control Money and Information* (2015). Soshana Zuboff (2019), investigadora y profesora en la Harvard Business School y autora del reciente libro *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019). Zeynep Tufekci (2017), profesora e investigadora en Ciencias de la Información y Biblioteconomía, y autora de *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (2017). Robert McChesney (2013), activista y profesor de Comunicación en la University of Illinois y autor de, entre otros libros *Digital Disconnect: How Capitalism is Turning the Internet Away from Democracy* (2013). Helen Nissembaum, cofundadora junto a Daniel C. Howe (2009; 2017) de iniciativas como TrackMeNot y AdNauseam y co-autora con Finn Brunton de *Obfuscation: A User's Guide for Privacy and Protest* (2015). Evgeni Morozov, escritor, periodista, investigador y profesor en varias universidades estadounidenses y autor de, entre otros, *The Net Delusion: The Dark Side of Internet Freedom* (2011). Cathy O'Neil, académica vinculada a la Columbia University, activista del movimiento Occupy Wall Street y autora de *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy* (2016). O Christian Fuchs, profesor de comunicación y medios en la University of Westminster, editor de la revista académica *tripleC: Communication, Capitalism & Critique* y coautor de *Digital*

Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data (Chandler y Fuchs, 2019).

Asimismo, se han generado numerosas iniciativas, proyectos y espacios de investigación dedicados al tema. Ejemplo de ello son: el Data Justice Lab, un centro de investigación de la Facultad de Periodismo, Medios y Cultura de la Cardiff University. Vinculado a este centro se desarrolla el proyecto *Data Justice: Understanding datafication in relation to social justice,* con Lina Dencik como investigadora principal. Arne Hintz, Lina Dencik y Karin Wahl-Jorgensen han publicado recientemente el libro *Digital citizenship in a datafied society* (2019). Otro ejemplo es el proyecto *Data activism: The politics of big data according to civil society*, encabezado por Stefania Milan y vinculado a la University of Amsterdam. Milan es autora de, entre otros, el libro *Social Movements and Their Technologies: Wiring Social Change* (2013). Por otra parte, existen iniciativas como el Public Data Lab, integrado por investigadores de diversas universidades europeas; la ONG británica Privacy International; el centro Eticas Foundation de investigación, formación y difusión del conocimiento sobre la tecnología big data y su impacto social, encabezado por Gemma Galdón Clavell (2018); o el Centre Internet et Société, vinculado al Centre National de la Recherche Scientifique (CNRS) francés, dirigido por Mélanie Dulong de Rosnay (2016) y Francesca Musiani (2017).

Entre las líneas de investigación más frecuentes de esta tendencia están: los riesgos de la datificación, la publicidad personalizada y el *profiling* (perfilación de los individuos); las relaciones del capitalismo y la vigilancia; la *plataformización* de la economía; los efectos de la automatización, la robotización, la inteligencia artificial y la cultura algorítmica; los problemas de discriminación y los sesgos provocados por las tecnologías de análisis de datos masivos, fundamentalmente relativos al género, la etnia, el país de origen o la clase social; el papel de los medios de comunicación en la conformación del discurso dominante; las actitudes y respuestas ciudadanas y las posibles formas de resistencia; las nuevas formas de gobernanza ciudadana y organización de los movimientos sociales y activistas basadas en el procesamiento de datos; las posibilidades y los límites de los marcos reguladores de protección de datos

personales y, en general, el papel de las instituciones públicas y la acción política; o las implicaciones para la justicia social y la democracia.

Por otra parte, muchos han destacado que este nuevo escenario de explotación de datos masivos supone un problema a nivel jurídico y político para la protección de la privacidad y de los datos personales. Con ello, se han incrementado también muy notablemente los estudios centrados en la teoría de la privacidad aplicados a las nuevas tecnologías digitales. En el mundo anglosajón, se conocen bajo el nombre de Filosofía y Derecho de la Privacidad (*Law and Philosophy of Privacy*). Entre las y los máximos exponentes de esta área, que tiene como referente el texto de 1890, *The Right to Privacy*, de Warren y Brandeis, están: Daniel J. Solove, profesor de Derecho en la George Washington University y autor de libros como *Nothing to Hide. The False Tradeoff between Privacy and Security* (2011) o *Understanding Privacy* (2008). Luciano Floridi, profesor de Filosofía y Ética de la información en el Oxford Internet Institute y autor de numerosos libros al respecto como *The Philosophy of Information* (2011), *The Ethics of Information* (2013) o *The Logic of Information* (2019). Anita Allen, profesora de Derecho y Filosofía en la University of Pennsylvania y autora de libros como *Unpopular Privacy: What Must We Hide?* (2011) e influyentes papers como *Coercing Privacy* (1999) o *Protecting One's Own Privacy in a Big Data Economy* (2006). Julie E. Cohen, profesora de Derecho de la tecnología en la Georgetown University y autora de varios libros, entre los cuales: *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (2012) o *Between Truth and Power: The Legal Construction of Informational Capitalism* (pendiente de publicación en octubre de 2019). O Amitai Etzioni, fue profesor de Sociología en la Columbia University y es autor de, entre otros, *The Limits of Privacy* (1999).

En un sentido amplio, estos estudios buscan concienciar y promover un debate público informado y basado en evidencias sobre las posibilidades y las consecuencias del desarrollo de las tecnologías *big data*. También sacar a la luz y anticipar los problemas derivados de las mismas y ofrecer conocimiento e indicaciones al respecto. Y, además, influir en la acción individual y organizada, pero también en las dinámicas de la política, el mercado y la propia academia respecto del uso de datos masivos.

Objeto de estudio, objetivos y metodología de la tesis

La presente tesis doctoral explora el impacto social y político de la explotación de datos masivos por parte de las grandes corporaciones tecnológicas a nivel europeo. Lo hace a través del análisis de algunos de los factores que determinan el contexto general en el que se produce esta explotación. La investigación tiene dos objetivos generales, que se desgranan en varios objetivos específicos.

El primer objetivo general es definir las características principales de dicho contexto [**OG1**]. Más concretamente, busca describir:

- El contexto tecnológico: la lógica de generación, recopilación y procesamiento de datos masivos [**OE1**].
- El contexto corporativo: las dinámicas del modelo de negocio de las grandes corporaciones tecnológicas en lo relativo a la explotación de datos masivos, y su encaje en el sistema económico actual [**OE2**].
- El contexto discursivo: los elementos centrales del discurso mediático predominante sobre el fenómeno y las tecnologías big data y los actores más influyentes en su conformación [**OE3**].
- El contexto social: las reacciones sociales mayoritarias ante la explotación de datos y las formas de resistencia promovidas por los sectores más concienciados e informados [**OE4**].
- El contexto jurídico: el modelo de protección que impone el Reglamento General de Protección de Datos (RGPD) (2016/679) a escala europea y su fundamentación teórica y conceptual [**OE5**].

El segundo es explicar cómo afectan estos cinco factores a la privacidad y a la libertad de la ciudanía europea y, de forma más específica, a su control sobre los datos **[OG2]**. Desglosado en función de los contextos analizados, el objetivo general 2 se codifica mediante la fórmula [**OG2–OE*n***].

- En el caso particular del contexto jurídico [**OG2–OE5**], se trata de evaluar en qué medida los mecanismos que establece el RGPD son eficaces para proteger a las personas del impacto de la explotación de datos masivos.

Para dar a respuesta los objetivos planteados, la tesis revisa, contextualiza y relaciona algunos de los estudios actuales más relevantes en ciencia y tecnología de datos, economía política de la comunicación, representación mediática de la tecnología emergente, recepción social del fenómeno big data y teoría de la privacidad. Estas aportaciones se examinan desde una posición teórica fundamentada, principalmente, en la teoría crítica del capitalismo (Federici, 2004; Fraser, 2012; 2017; Harvey, 2005), la teoría política feminista (Hanisch, 1970; Pateman, 1989; Young, 1987) y la filosofía republicana (Pettit, 1996; 1997; 2010; 2012). Además, presenta dos estudios empíricos sobre el discurso mediático en torno a la tecnología big data, desde la teoría del *framing* (Entman, 1993; Goffman, 1975) y el análisis cuantitativo de contenido. Asimismo, ofrece un análisis teórico-conceptual del reglamento europeo de protección de datos.

La tesis consta de un compendio de cinco artículos publicados (o aceptados para su publicación). La Tabla 1 (a continuación) muestra los objetivos específicos a los que responde cada uno de ellos, así como las metodologías utilizadas.

Esta memoria, realizada en la fase final de la tesis, organiza y enlaza las aportaciones más destacadas de las publicaciones, las analiza desde una perspectiva teórica unificada y refuerza ciertos aspectos que las publicaciones han reflejado de forma menos explícita, debido a su especificidad. Se divide en dos grandes capítulos, separados por el compendio de artículos. El primero define el contexto tecnológico, corporativo, discursivo, social y jurídico de la explotación big data en Europa. Introduce, además, las ideas de las teorías feminista y republicana que se trabajan a lo largo de la tesis. El segundo discute los aspectos centrales de cada uno de los cinco contextos analizados en el primer capítulo y los artículos, para explicar el impacto de la explotación de datos masivos. Las conclusiones recogen, de forma resumida, los puntos más destacados de la tesis.

Aunque la tesis incluye dos estudios empíricos, su principal aportación es teórica. Esto no quiere decir que el objetivo sea desarrollar una teoría original o sistematizar la realidad de una forma nueva. Que la aportación sea teórica significa que permite identificar y comprende las implicaciones sociales y políticas de la explotación de datos masivos, en base a un análisis razonado y novedoso del contexto en el que se produce dicha explotación.

Tabla 1. Objeto de estudio, relación de objetivos específicos y metodología de las publicaciones del compendio[2]:

	Objeto de estudio	Objetivos	Metodología
1. La conversación sobre big data en Twitter. Una primera aproximación al análisis del discurso dominante.	Discurso predominante sobre big data en Twitter.	[OE1, OE3, OG2–OE3]	Análisis cuantitativo del contenido de una muestra de 162.007 *tweets* publicados entre el 23 de noviembre y el 22 de diciembre de 2013, que contienen el concepto "*big data*" o el hashtag *#bigdata*.
2. Tay is you. The attribution of responsibility in the algorithmic culture.	Discurso predominante sobre el caso del chatbot *Tay* en la prensa digital.	[OE1, OE2, OE3, OG2–OE1,2y3]	Discusión teórica sobre las nociones tradicionales de responsabilidad y rendición de cuentas aplicadas al "comportamiento" del chatbot Tay. Estudio de la representación mediática del caso mediante un análisis de *frames* de las noticias publicadas en la prensa digital entre abril y noviembre de 2016, realizado en base a la categorización de Semetko y Valkenburg (2000).
3. Big social data: límites del modelo *notice and choice* para la protección de la privacidad.	Eficacia del modelo de la notificación y el consentimiento para la protección de datos.	[OE1, OE2, OE4, OE5, OG2–OE1,2,4y5]	Análisis razonado del modelo de la notificación y el consentimiento, en relación a la lógica de procesamiento de datos masivos.
4. Your likes, your vote? Big personal data exploitation and media manipulation in the US presidential election campaign of Donald Trump in 2016.	Condiciones de posibilidad del caso Facebook - Cambridge Analytica.	[OE1, OE2, OE4, OE5, OG2–OE1,2y5]	Estudio de los contextos científico-tecnológico, empresarial y legal en los que se produce el caso Facebook-Cambridge Analytica, a partir de las filtraciones mediáticas y las investigaciones científicas relacionadas con el caso.
5. Personal data are political. A feminist view on privacy and personal data protection [*en edición*].	Pertinencia de la fundamentación teórica y conceptual del modelo de protección de datos en Europa.	[OE1, OE2, OE4, OE5, OG2–OE1,2,4y5]	Discusión sobre las concepciones de privacidad y de libertad subyacentes al reglamento europeo de protección de datos personales, desde la perspectiva de la crítica feminista de segunda ola a la privacidad (Hanisch, 1970) y la teoría republicana de libertad como *no-dominación* (Pettit, 1997; 2012).

[2] El listado de las publicaciones del compendio y sus datos referenciales y de indexación se presentan en la página 51.

El contexto de la explotación big data

Este capítulo tiene el propósito de definir el contexto general en el que se integra la explotación big data [**OG1**]. Para ello se divide en siete secciones que organizan y relacionan las principales aportaciones de la tesis a la comprensión de: la lógica de generación, recopilación y procesamiento de los datos masivos [**OE1**]; las dinámicas del modelo de negocio de las grandes corporaciones de servicios digitales y su encaje en el sistema económico capitalista [**OE2**]; el marco del discurso mediático predominante sobre las tecnologías big data [**OE3**]; las reacciones sociales mayoritarias y las formas de resistencia a la explotación que proponen los sectores especializados [**OE4**]; y el modelo jurídico de protección de datos que establece el RGPD a escala europea [**OE5**]. Este capítulo incluye, además, la explicación de dos teorías críticas con la naturaleza de la fundamentación conceptual del reglamento, que servirán de base metodológica para el posterior cumplimiento del objetivo general 2: la crítica feminista a la privacidad y la teoría republicana de libertad.

[OE1] Lógica big data

Muchas de nuestras acciones, tanto en el entorno digital, como en el analógico, se registran en datos. La introducción de internet y especialmente las redes sociales y de los dispositivos móviles ha generado importantes cambios en la forma tradicional de compartir, de comunicarse, y también de acceder a servicios básicos (boyd y Crawford, 2011). Esta sección explica la lógica de generación, recopilación y procesamiento de datos masivos.

Datificación y digitalización

En la actualidad, resultaría complicado llevar una vida normal en un país europeo sin utilizar un ordenador o un dispositivo móvil, Google para buscar información de cualquier tipo, las redes sociales para conocer gente o mantener el contacto con los amigos y familiares, Amazon para comprar un producto que no se vende cerca de tu casa, o la banca electrónica para consultar los últimos movimientos en tu cuenta bancaria. Son solo algunos ejemplos. Pero, más allá de estos servicios nacidos en el

entorno digital, otros servicios básicos como el transporte urbano, las redes de gas y electricidad o la gestión de información en la sanidad pública también han sido digitalizados. Esta nueva mediación digital, ha provocado que la *datificación* de la vida cotidiana sea una tendencia en alza (Mayer-Schönberger y Cukier, 2013).

Todos estos datos permitirían a un observador determinar, de forma más o menos detallada, los comportamientos, características, intereses y preferencias personales de los individuos a los que se refieren. Pero también definir el entorno de esos individuos y las personas que forman parte de él (boyd, Levy y Marwick, 2014). En este sentido, el caso de los "perfiles sombra" (en inglés, *shadow profiles*) ha demostrado que plataformas como Facebook pueden trazar un perfil más o menos preciso sobre una persona, aunque esa persona no haya sido nunca usuaria de ellas, gracias a la información que otras personas difunden sobre ella (Sarigol, García y Schweitzer, 2014).

El caso de los metadatos añade todavía más complejidad. Son datos sobre el contexto en que se generan los datos —como la localización, la hora, el lenguaje utilizado, o el tipo de dispositivo utilizado, por poner algunos ejemplos—. Se generan por defecto al utilizar un producto o un servicio, o al interactuar con otras personas que lo utilizan (Tufekci, 2017).

<u>De la pre-clasificación al filtrado</u>

El gran aumento de los datos ha obligado a repensar las técnicas de recopilación y de tratamiento. La analítica big data no deja de ser una forma de análisis cuantitativo más desarrollada. No obstante, conlleva importantes novedades con respecto a las técnicas tradicionales.

En primer lugar, la recopilación de los datos es masiva e indiscriminada (Baruh y Popescu, 2017). Tradicionalmente primero se definía qué tipo de datos interesaría analizar, para determinar cuáles era necesario recopilar. Es decir, se realizaba una preclasificación de los datos que después se buscarían y se almacenarían. Por el contrario, las técnicas de minería de datos masivos se caracterizan por recoger conjuntos completos de información y, posteriormente, aplicar filtros de búsqueda que permiten separar aquellos que interesa analizar en un momento determinado.

De este modo, la analítica big data supera en gran medida la necesidad de trabajar sobre una muestra representativa, gracias a la posibilidad de acceder a volúmenes muy elevados de datos sobre un universo de estudio, pese a que el formato, origen y contenido de los mismos sea muy diverso (Manovich, 2012). Mayer-Schönberger y Cukier (2013: 12-13), se han referido a la selección muestral como "an artefact of a period of information scarcity, a product of the natural constraints on interacting with information in an analog era".

Agregación y automatización

Dado que los datos masivos sobrepasan la capacidad de análisis humana, una vez almacenados, se procesan mediante sistemas automatizados, diseñados para realizar análisis cuantitativos complejos (boyd y Crawford, 2011). El tratamiento se realiza sobre conjuntos de datos agregados, que permiten vislumbrar atributos y patrones latentes en ellos y, por tanto, inferir información que las personas no han difundido de forma explícita (Baruh y Popescu, 2017; Tufekci, 2014). Como consecuencia, el análisis combinado de un conjunto masivo de datos que aislados no son "personales", permite obtener de ellos información que sí podría serlo.

Un ejemplo de esto son los estudios psicométricos desarrollados por investigadores de la Universidad de Cambridge (Kosinski, Stillwell y Graepel, 2013; Stillwell y Kosinski, 2012; y Youyou, Kosinski y Stillwell, 2015) que fueron utilizados en el escándalo de corrupción de datos perpetrado por Cambridge Analytica y Facebook (véase: Cadwalladr, 7 de mayo de 2017; Cadwalladr, 17 de marzo de 2018; Cadwalladr y Graham-Harrison, 17 de marzo de 2018; Rosenberg, Confessore y Cadwalladr, 17 de marzo de 2018). En concreto, el trabajo publicado por Kosinski, Stillwell y Graepel (2013) demuestra que, a través del análisis automático de la reacción *like* ("me gusta") de una persona a los contenidos publicados en Facebook, es posible predecir algunos de sus atributos personales tan sensibles como: su género, su etnia, su orientación sexual, política y religiosa, o información relativa al consumo de drogas o su nivel de satisfacción con la vida, entre otros.

Reaccionar a una publicación pulsando el botón "me gusta" es el tipo de interacción básica que una persona usuaria ejerce en una plataforma como Facebook. Es, al mismo

tiempo, una acción que no parece difundir una información demasiado comprometida: en principio, mostrar "a los demás" que algo te gusta, te disgusta, o te llama la atención, no resulta demasiado comprometedor. Además, los *likes* son, como subrayan Kosinski, Stillwell y Graepel, registros digitales del comportamiento humano muy fácilmente accesibles y, a menudo, "públicos". Es decir, que no hace falta tener un perfil en Facebook, ni estar en contacto con la persona que emite el *like*, para poder verlo.

En esta misma línea, varios estudios realizados en la red social Twitter (Guerrero-Solé, 2017; 2018; Guerrero-Solé, Corominas-Murtra y Lopez-Gonzalez, 2014; Guerrero-Solé y Lopez-Gonzalez, 2019) demuestran que es posible predecir la indecisión de los votantes y sus preferencias por los pactos y coaliciones tras las elecciones a través del análisis de sus *retweets* (de nuevo, una acción básica en el uso de la plataforma). En concreto, las investigaciones prueban que esta predicción es posible si se analizan las superposiciones entre los grupos de personas que retuitean los mensajes emitidos por los usuarios más influyentes de diferentes opciones políticas (*RON*: *retweet overlap network*) durante un periodo electoral.

Estos estudios permiten observar algunas de las posibilidades de la analítica big data. Pero, cabe destacar, que el objetivo principal de estas técnicas no es utilizar esta información vinculada a la identidad de personas concretas. Desde Facebook (Facebook for Business, 8 de mayo de 2014), por ejemplo, se ha declarado que el propósito de sus análisis de datos masivos no es vigilar la actividad individual, sino extraer información valiosa del conjunto de las expresiones colectivas. De hecho, otro de los mayores distintivos de la analítica big data es que permite encontrar similitudes entre las personas, gracias al análisis de sus características o comportamientos, para "categorizarlas" como parte integrante de grupos sociales o fenómenos más amplios (boyd, Levy y Marwick, 2014). Esto abre, a su vez, la posibilidad de analizar rasgos definitorios de dichos grupos o estudiar fenómenos a gran escala (Halavais, 2015).

Por otra parte, la automatización de los procesos se fusiona con la autonomía de la técnica y establece una estrecha relación entre los datos masivos, el uso de algoritmos y la inteligencia artificial (véase: Marsland, 2015; Mattelart y Vitalis, 2015; Shalev-Shwartz y Ben-David, 2014). El término "cultura algorítmica", así definido por Hallinan y Striphas (2016: 119), denomina un nuevo escenario caracterizado por "the use of

computational processes to sort, classify, and hierarchize people, places, objects, and ideas, and also the habits of thought, conduct, and expression that arise in relationship to those processes".

A toda esta complejidad de la lógica big data se suma que, tanto las técnicas de análisis los datos, como los procesos algorítmicos que las acompañan son especialmente opacos (Caplan y boyd, 2016; Kroll *et al*., 2017). Frank Pasquale (2015) es conocido por sus investigaciones sobre este tema. Pasquale explica que esta opacidad tecnológica es el resultado de una forma de producción estructural de ignorancia relacionada con el secretismo real, el secretismo jurídico y la ofuscación intencionada, que fomentan corporaciones y gobiernos.

[OE2] El negocio de los datos

Hoy, la explotación de datos masivos tiene dos objetivos principales: el beneficio económico y el control social. El primero suele atribuirse a las empresas y a los mercados (en un sentido amplio, los poderes privados), mientras que el segundo, al ejercicio de las instituciones y gobiernos (poderes públicos). A pesar de ello, la relación entre ambos objetivos no es excluyente y su alcance actual no sería posible sin una colaboración entre los poderes públicos y los privados (Morozov, 2011).

Un aspecto central para entender esta cuestión es que, durante las últimas décadas, ha emergido y se ha consolidado un tipo de empresa tecnológica centrada en la oferta de servicios digitales, cuyo modelo de negocio se basa en la explotación de datos masivos. En el centro de este sector están los "gigantes digitales", también conocidos como GAFAM (Google, Apple, Facebook, Amazon y Microsoft). Estos recopilan la gran mayoría de los datos digitales que difunden millones de personas a diario (Tufekci, 2017). Las expresiones "big social data" (Halavais, 2015) o "social media big data" (Tufekci, 2014), hacen referencia a los datos que las personas difunden a través de estas plataformas "sociales", generando una huella digital resistente (Burkell, Fortier, Cheryl, Yeung Cheryl Wong y Simpson, 2014).

La economía política de la comunicación estudia las estructuras de mercado, las instituciones y las prácticas que definen los sistemas comunicativos y mediáticos y

examina cómo estos se relacionan con el poder económico y político de las sociedades en las que se integran, y si refuerzan o debilitan los sistemas democráticos. Según McChesney (2013), cómo y por qué los "gigantes digitales" han conseguido situarse entre las empresas más importantes en la economía mundial tiene que ver con cómo es el internet de hoy. Internet nació con la promesa de ser una esfera pública abierta, ajena a las lógicas del mercado, que daría un poder y unas herramientas sin precedentes a la ciudadanía. Muchos lo imaginaban como un elemento democratizador del acceso al conocimiento y a la información que ayudaría a superar las desigualdades sociales. También se esperaba que contribuyese a aumentar la competitividad de los mercados, la responsabilidad y la rendición de cuentas de las empresas, y la transparencia y participación en las acciones de los gobiernos e instituciones públicas. McChesney explica que esta promesa, sin embargo, ha sido comprometida por las fuerzas capitalistas que han convertido internet en una esfera cada vez más controlada por un mercado propietario y monopolístico.

En el entorno de internet hay, al menos, tres dinámicas estrechamente relacionadas entre sí que hacen que el negocio de los gigantes digitales tienda al monopolio: los *network effects* (en castellano, efectos de red), la publicidad basada en datos como principal fuente de ingresos y la importancia de los estándares técnicos.

Los efectos de red

La primera de ellas, los efectos de red (*network effects*) se refieren al principio por el cual, cuántas más personas forman parte de una red, más atractiva y más útil es esta red para otras personas, al mismo tiempo que los costes de exclusión aumentan para quienes no forman parte de ella (Bartlett, 2018; Lanier, 2018; McChesney, 2013; Tufekci, 2017).

Esta dinámica tiene una repercusión clara en la experiencia de una persona dentro de esa red. Por otra parte, cuantos más integrantes tiene una red y cuanto mayor es su interacción, más información tiene quien la maneja para, entre otras cosas, mejorar su servicio. Plataformas sociales como Google o Facebook son las que más se benefician de estos efectos, dado que sus servicios se basan en promover la interacción entre personas y con contenidos que puedan ser de su interés (Tufekci, 2017). La precisión

del algoritmo de recomendación de Google, por poner un ejemplo, mejora paralelamente al aumento de personas que utilizan el buscador (McChesney, 2013). De la misma manera, plataformas de contenido a demanda como Netflix o Amazon, registran en datos todas las acciones de sus usuarios (Antunes y Maia, 2018), con el objetivo de mejorar la experiencia del usuario mediante la recomendación y la oferta constante de contenidos híper personalizados (Fernández-Manzano, Neira y Clares-Gavilán, 2016; Mendiratta, Wong, Grimm, Yogeshwar y Archiquette, 2015).

Cuando se inicia esta dinámica, las potenciales redes alternativas a la predominante tienden al fracaso, por el simple hecho de que las utiliza menos gente. Por este motivo, Lanier (2018: 21) también utiliza la expresión *lock-in* (en castellano, encierro) para referirse a estos efectos de red. A esto se suma que los efectos de red no favorecen a las compañías en el momento de su lanzamiento al mercado. Por ello, aunque su éxito o su fracaso depende, también, de la calidad de sus servicios (Tufekci, 2017) este está fuertemente determinado por el capital de partida de la compañía (McChesney, 2013).

Esto genera una inercia por la cual la compañía más rica se hace cada vez más rica (y tiene cada vez más control sobre los datos), mientras que el resto se enfrenta a grandes y crecientes barreras de entrada y se empobrece debido a los acelerados costes de la exclusión. En palabras de McChesney (2013: 132): "The largest firm in an industry increases its attractiveness to consumers by an order of magnitude as it gets a greater market share, and makes it almost impossible for competitors with declining shares to remain attractive or competitive." Con ello, la supuesta competitividad del mercado y su pretendida capacidad para imponer restricciones al poder de las compañías más ricas quedan muy limitadas (Tufekci, 2017). Bartlett (2018), explica que esto supone, además, que las grandes empresas pueden presionar o absorver a otras más pequeñas sin asumir riesgos, sobre todo si estas últimas dependen de alguna manera de ellas, y así incrementar su poder en el mercado y también sus fuentes de datos. En los últimos años, por ejemplo, Facebook ha comprado Instagram (en 2012) y WhatsApp (en 2014), dos redes sociales notablemente al alza.

La publicidad basada en datos

Si hablamos de la tendencia al monopolio de los gigantes digitales, el segundo factor a destacar es la predominancia de la publicidad basada en datos como una fuente de ingresos principal (Tufekci, 2017).

La globalización y la irrupción de los medios sociales han roto con el paradigma de comunicación unidireccional (Castells, 2009). Por otra parte, el desgaste de la confianza ciudadana en los medios de comunicación tradicionales, ha llevado a muchas personas a dejar de utilizarlos para consumir contenidos e informarse en internet (Marwick y Lewis, 2017).

Por todo esto, se ha generado una nueva necesidad de interaccionar en línea, de forma constante y personalizada con el público objetivo (Neff y Nagy, 2016). El análisis de datos masivos permite generar estrategias comunicativas y publicitarias personalizadas más eficaces, capaces de mejorar las tasas de interacción del público con esos mensajes (Liu y Yi, 2017). En particular, la información que se extrae de las plataformas sociales tiene una enorme relevancia para el sector publicitario, en tanto que en ellas se registran las opiniones y las respuestas de los usuarios ante temas, servicios o productos concretos (Nair, Shetty y Shetty, 2017). Esto permite analizar las reacciones (también las emocionales) del público y adaptar los mensajes en tiempo real (Li, Wang, Zeng y Yuan, 2013).

Redes sociales como Facebook, por ejemplo, se financian básicamente a través de la publicidad que se emite en sus plataformas. Como explica Tufekci (2017), la única manera de aumentar el precio que los anunciantes pagan por publicitarse en sus espacios es ofrecerles la posibilidad de que estos anuncios sean lo más personalizados que sea posible, en base a los datos de las personas usuarias del servicio. Solo las plataformas más exitosas son capaces de recopilar cantidades de datos suficientemente grandes sobre los intereses, las preferencias y los comportamientos específicos de sus usuarios, como para que esta publicidad sea más efectiva. De nuevo, cuantas más personas utilizan un servicio, más datos tiene la compañía que lo proporciona y más caros puede vender sus espacios publicitarios. Aquellos servicios que cuentan con un mayor número

de usuarios, ganan la mayoría del dinero que genera la publicidad digital. Ni siquiera Twitter, señala Tufekci, es suficientemente grande para ello.

En esa línea, McChesney (2013) señala que la computación en la nube es un punto clave para que los gigantes digitales excluyan del mercado a otras empresas más pequeñas. Esta forma de almacenamiento permite a las empresas acumular enormes cantidades de datos en sus servidores, pero las infraestructuras y los sistemas necesarios para disponer de ella tienen un alto coste inicial.

La importancia de los estándares técnicos

En tercer lugar, los estándares técnicos son indispensables para homogeneizar la legibilidad y la usabilidad de los servicios digitales para todas las partes. Por lo tanto, explica McChesney (2013), la compañía que consigue que sus sistemas se conviertan en la referencia de la industria se sitúa en una posición privilegiada desde la cual puede influir en las invenciones futuras que podrían afectar su modelo de negocio. Esta es la razón por la cual las patentes han adquirido un papel tan importante para el modelo de negocio de los gigantes digitales. Un ejemplo de ello es el caso de Google, Microsoft o Apple, que desarrollan sistemas operativos (Android, Windows o iOS), navegadores (Google Chrome, Internet Explorer o Safari) o buscadores web (Google o Bing).

Estos tres factores tienen como consecuencia que, tanto el valor económico de los datos que recopilan los gigantes digitales, como su valor para conocer y definir a la sociedad, aumentan exponencialmente. Con ello, queda de manifiesto que, comenzar a tratar los datos como bienes "transferibles", introduciéndolos en el ámbito del mercado y allanando el camino para especular con su "precio", ha sido fundamental para el éxito de su negocio. Esta parece ser también una explicación lógica a la fuerte opacidad de las operaciones de estas compañías en lo relativo al procesamiento de datos.

Todo ello, sumado a las lógicas de generación, recopilación y procesamiento de las tecnologías big data, provoca lo que, en los términos de Federici (2004), sería una forma de "mecanizar" la "producción" y la "reproducción" de la riqueza, distintiva del sistema capitalista desde sus orígenes. En primer lugar, mediante la creación de escenarios que dan lugar a la conversión de la actividad humana en datos digitales y la sistematización de su procesamiento. En segundo, mediante la reconfiguración de las relaciones de

poder y la estabilización de una concepción de las personas como agentes productores de datos.

En esta línea, Zuboff (2019) argumenta que los humanos son la fuente de una nueva materia prima (los datos) que alimenta una estructura paralela al capitalismo económico que ella denomina "capitalismo de la vigilancia". Los capitalistas de la vigilancia, explica Zuboff, han incorporado los datos a las dinámicas del mercado, mercantilizando así las vidas privadas de las personas, con el único propósito de abrir el camino a nuevas formas de enriquecerse. Una de las mayores diferencias de esta forma de capitalismo de la vigilancia es, según Zuboff, que ya no es un capitalismo enfocado en las personas. Los principales clientes de compañías como Facebook o Google no son sus usuarios, sino otras empresas e instituciones que desean utilizar los datos que estas recopilan, o los servicios y tecnologías que desarrollan.

No obstante, quizás sin necesidad de pensar en un capitalismo de una naturaleza diferente, las prácticas de las grandes corporaciones tecnológicas se inscriben en lo que muchos han definido como una nueva expresión de un capitalismo depredador y financierizado, que apenas produce riqueza, sino que la expropia y la redistribuye en su beneficio (Arruzza, Bhattacharya y Fraser, 2019; Fraser, 2017; Harvey, 2005). Harvey (2005: 159) utiliza el término "acumulación por desposesión" para referirse a "the continuation and proliferation of accumulation practices which Marx had treated of as 'primitive' or 'original' during the rise of capitalism". Dos mecanismos fundamentales de esta forma de acumulación de la riqueza son la *financierización* —la apropiación de valor mediante la depredación y la especulación— y la *privatización* y *mercantilización* de todo tipo de bienes que no eran mercancías —con lo que los diferentes derechos de propiedad se convierten en derechos exclusivos de propiedad privada—. Según Harvey, la globalización y los sistemas políticos neoliberales han impulsado esta nueva forma de acumulación capitalista al situar las corporaciones y servicios financieros en un lugar central de la economía moderna. En los sectores financieros, el empleo crece rápidamente, dando una impresión de dinamismo de la economía. Pero gran parte del negocio de las finanzas es puramente especulativo, con lo que son negocios inestables y su productividad es dudosa.

Estos cambios en la economía, explica Harvey, han venido acompañados de un gran aumento de la inversión pública en las tecnologías de la información, no de forma casual. La tecnología de la información, dada su inmaterialidad, es una tecnología privilegiada por el neoliberalismo: "is far more useful for speculative activity and for maximizing the number of short term market contracts than for improving production." (Harvey, 2005: 159),

Co-dependencia

El potencial de los datos masivos ha generado fuertes intereses compartidos entre los gigantes digitales y los poderes públicos. Así, el monopolio de los gigantes digitales tampoco sería posible sin, al menos, un factor más: la creciente cooperación entre ambos (Bartlett, 2018; McChesney, 2013; Morozov, 2011).

Por un lado, los gobiernos, los ejércitos o las agencias de seguridad nacional ganan acceso a una información de la que disponen estas compañías, que no podrían obtener por otras vías, y de la cual dependen cada vez más para operaciones de inteligencia o de vigilancia interna. Además, y pese a que estas empresas son conocidas por pagar bajos impuestos en los estados europeos y de domiciliarse en aquellos países con unos regímenes tributarios más favorables, su peso en el conjunto de la economía global las hace ya "too big to (let) fail" —utilizando la expresión de Sorkin (2009), después revisada por Lin (2012): "demasiado grandes como para dejarlas quebrar"—.

Por otro lado, el enriquecimiento de compañías como Google, Facebook o Amazon depende, en gran medida, de las políticas impositivas y de las legislaciones europeas y estatales. Por lo que no está en sus intereses enemistarse, sino colaborar, con las autoridades públicas. Esto les permite, además, beneficiase de fuentes de ingresos públicos y mantener una vinculación con el desarrollo de la tecnología militar, que en muchos casos es explotada con fines comerciales (McChesney, 2013; Morozov, 2011).

Esta colaboración, además de revertir en decisiones políticas favorables a los intereses del mercado de datos, genera una posición de superioridad de los poderes económicos frente a los democráticos (Morozov, 2011). Según Bartlett (2018), las grandes corporaciones tecnológicas tienden a distorsionar la política utilizando su poder económico para ejercer presión en favor de sus intereses. En palabras de McChesney

(2013: 142): “None of these monopolies would have been possible without supportive and enabling government policies on a range of issues, as well as considerable previous investments by the government”.

Casos como el revelado por Snowden en 2013, el de Cambridge Analytica o el del iPhone de San Bernardino, han confirmado que los datos que recopilan estas compañías ya están siendo utilizados para operaciones de vigilancia interna, como arma electoral (tanto en Europa como en Estados Unidos) o en casos de crimen y terrorismo. De forma particular, el caso del iPhone de San Bernardino muestra claramente que un conjunto de información que no fue recolectada al principio por una empresa para investigar profundamente a una persona concreta, puede ser eventualmente usada para hacerlo.

Esta creciente dependencia forma parte de la tónica general propia de un mundo capitalista globalizado, en el cual los poderes públicos están cada vez más supeditados al sector privado. Feenstra (2018) utiliza la metáfora *kidnapped democracy* (en castellano “democracia secuestrada”)[3] para definir un escenario en el cual las élites financieras han alcanzado un poder que les permite imponer y determinar decisiones políticas en su beneficio y, al mismo tiempo, limitar el poder de las estructuras democráticas básicas y la voz política de los ciudadanos. Según Feenstra, estas élites “secuestradoras” del sistema político democrático se caracterizan por ser particularmente silenciosas. No generan alerta sobre sus acciones, ni reclaman abiertamente un rescate. Su poder consiste, precisamente, en que su control sobre las instituciones pase inadvertido, para generar la apariencia de que, si las democracias pierden poder, no es porque otros actores se estén apropiando de él para satisfacer sus intereses privados.

Silvia Federici en una conversación con Astra Taylor (junio de 2019) afirma que la democracia vive una crisis causada por el sistema económico imperante. Federici argumenta que el capitalismo actual no supone una ruptura ni una novedad con su historia, sino que es la consecuencia de un desarrollo que lo ha vuelto cada vez más “puro”. Ahora, los capitalistas no necesitan la mediación del estado para imponerse. De acuerdo con la filósofa, para entender cómo se ha llegado a este punto debemos atender

[3] Esta metáfora da título a un nuevo libro de Feenstra, *Kidnapped Democracy*, todavía pendiente de ser publicado en el mes de noviembre de 2019.

a tres factores sucesivos: En primer lugar, el fin del Fordismo. En segundo, el momento en que los estados comenzaron a estar representados por agencias mundiales como el Banco Mundial. El tercero es el que vivimos actualmente. Un momento en el cual estas agencias están siendo reemplazadas por la actuación directa de las grandes corporaciones internacionales. Con ello, los centros de poder se han vuelto lejanos a la ciudadanía y el poder se ha vuelto más impersonal, más abstracto y más independiente.

[OE3] El discurso mediático

Autores como Lippmann (1998) o Herman y Chomsky (2002) han dedicado parte de su trabajo a estudiar el rol de los medios de comunicación en la transmisión y la aceptación social de los intereses de los grupos de poder. De acuerdo con Lippmann (1998: 248), los medios contribuyen a la "fabricación" del consentimiento social ante estos intereses privados. Esto, dice "is a very old one [*art*] which was supposed to have died out with the appearance of democracy. But it has not died out. It has, in fact, improved enormously in technic, because it is now based on analysis rather than on rule of thumb." Partiendo de una crítica a la concepción antidemocrática de la sociedad de Lippmann, Herman y Chomsky (2002) toman esta idea de la creación de consentimiento para su *propaganda model*. En él explicaron cómo los medios de comunicación, dada su dependencia de las fuerzas del mercado, las asunciones de los mismos periodistas y la autocensura, generan un clima social que favorece que las personas consientan ante ciertas políticas que, en un escenario diferente, no consentirían. Klaehn *et al*. (2018) han remarcado la relevancia de este modelo de propaganda en el contexto social, tecnológico y mediático de hoy. En esta línea, Stahl (1995) describe el "poder ideológico" de los medios de comunicación como su capacidad para desempeñar dos funciones: ayudar a construir una cierta realidad y legitimar y atribuir autoridad a los poderes ya consolidados.

Esta construcción mediática de la realidad no tiene tanto que ver con la imposición de un discurso pretendidamente manipulador o falso, sino más bien con la atribución de relevancia a ciertas interpretaciones y valoraciones en detrimento de otras. Es decir, con llamar la atención sobre ciertos aspectos de la realidad, e infrarrepresentar otros

(Lawrence, 2000). El *framing* (enmarcado) es una de las principales técnicas por medio de las cuales los medios contribuyen a que la realidad se interprete de una forma determinda (Entman, 1993; Marwick y Lewis, 2017). Los marcos interpretativos, o *frames*, sirven para definir situaciones y dar sentido a la realidad, permitiendo que las personas las comprendan y se comporten en consecuencia (Goffman, 1975). Kahneman y Tversky (1984) mostraron el poder de los *frames* sobre las actitudes y los comportamientos de las personas.

La representación mediática de la tecnología

En el caso de la representación mediática de las tecnologías, Druckman y Bolsen (2011) han argumentado cómo el éxito o el fracaso de una tecnología emergente depende, en gran medida, del clima de opinión pública que fomenta los marcos interpretativos mediáticos en torno a ella. A este respecto, Spicer (2005) defiende que, el uso de las tecnologías digitales no viene determinado por el diseño de la tecnología en sí misma, sino que se conforma durante su proceso de introducción social. Un proceso a menudo fuertemente marcado por la movilización de los discursos interesados de las fuerzas económicas y políticas.

En la década de los 90, Stahl (1995) condujo un importante estudio, que analizó la representación mediática realizada por la revista *Time* durante diez años sobre los primeros ordenadores personales de IBM. Sus resultados muestran que las noticias hicieron un uso extremadamente recurrente del lenguaje mágico y religioso. Además, explica, los ordenadores fueron frecuentemente retratados (personificados) como la parte activa en las relaciones humano-máquina. Una evidencia que Stahl (1995: 252) interpreta como parte de un interés subyacente por legitimar la opacidad de esta nueva tecnología: “Computers are powerful but also mysterious. Their power is ours but not to undersand.” Argumenta que, en este sentido, la contribución mediática al discurso público sobre la tecnología tiende a ceñirse y a estabilizar el discurso promocionado por el mercado. Es decir: a promover su definición sobre la tecnología, sin introducir demasiado debate o tensiones al respecto. Algo que Stahl considera que se debe, en parte, a que no todos los actores sociales están igualmente capacitados para hacer esta definición.

Uno de los estudios más relevantes al respecto de la representación mediática del fenómeno big data es el desarrollado por Puschmann y Burgess (2014). Apunta que, tal y como ha ocurrido tradicionalmente con otras tecnologías o descubrimientos científicos emergentes, el discurso mediático sobre big data es generalmente confuso impreciso y sesgado, y está determinado por las disputas de poder sobre el valor de los datos. El análisis de estos investigadores muestra un uso excesivo de metáforas y términos "familiares" que han provocado una híper simplificación del fenómeno. Esto, lejos de ayudar a su comprensión por parte de la ciudadanía, genera confusión. Además, señala que, de forma generalizada, los medios han contextualizado los datos como una mercancía "consumible" y "valiosa", y los procesos de explotación de los mismos como algo "natural" e "inevitable".

[OE4] Reacciones y resistencias sociales

Este escenario ha tenido una respuesta por parte de la ciudadanía, que aunque no refleja una clara oposición a la explotación de datos masivos, sí deja ver un cierto descontento. Lo reflejan diferentes encuestas y estudios realizados en los últimos años.

Respuestas paradójicas

En España, un barómetro emitido por el Centro de Investigaciones Sociológicas (CIS) en febrero de 2017, recoge que a un 76% de los españoles les preocupa mucho o bastante la protección de los datos personales y el posible uso de información por otras personas, especialmente en internet y las redes sociales. A nivel europeo, un Eurobarómetro especial sobre protección de datos (Special Eurobarometer 431, Junio 2015) refleja que menos de un 25% de los ciudadanos europeos confía en las empresas proveedoras de servicios digitales como las redes sociales o los motores de búsqueda. Un 71% considera que ceder su información personal es parte intrínseca de la vida moderna y un 58% que no existe alternativa a hacerlo si quieren utilizar productos o servicios.

Pese a estar preocupadas por la privacidad de sus datos personales, diferentes estudios muestran que, en general, las personas siguen utilizando servicios y productos digitales

y difundiendo información de una forma aparentemente despreocupada, especialmente en el ámbito de internet y las redes sociales. Esta disonancia tiene el nombre de "paradoja de la privacidad" (Barnes, 2006). La mayoría de autores han buscado la explicación a esta paradoja en características y circunstancias individuales de las personas (Barnes, 2006; Taddicken, 2014). Sin embargo, otros (como Hargittai y Marwick, 2016; o Turow, Hennessy y Draper, 2015) han apuntado la posibilidad de que el origen no se encuentre a nivel individual. La pregunta es: ¿cómo debemos interpretar estas contradicciones? ¿Se deben a una falta de preocupación por la privacidad o la protección de los datos personales? ¿Son resultado de la ignorancia, la conformidad o la irresponsabilidad individual? ¿Pueden tener que ver con una imposibilidad para actuar de acuerdo con las propias convicciones?

Cuando se pregunta a las personas qué les preocupa exactamente de su privacidad, muchas responden que, en realidad, "no tienen nada que ocultar". Este argumento ha sido analizado por Solove (2011). La respuesta pone de manifiesto que muchas personas entienden los asuntos privados como algo que ocultar "a los demás", o que debe ser "secreto". Lo llamativo, es que responden de este modo cuando se les pregunta por la explotación de datos masivos realizada por grandes corporaciones o gobiernos. Esto demuestra que, como es probable que ningún otro humano llegue a ver esa información, o a utilizarla para una finalidad pública, entonces la referencia a la privacidad resulta confusa, y las personas acaban afirmando que la situación no supone un problema.

Otra reacción contradictoria a esta situación, que puede aportar un poco de luz sobre esto es la "paradoja del conocimiento" (Baruh y Popescu, 2017). Esta paradoja describe la situación de aquellas personas bien informadas y altamente concienciadas sobre los riesgos de la explotación de datos, que, pese a intentar protegerse, se sienten incapaces de hacerlo.

Suicidio digital

A menudo, la paradoja del conocimiento da lugar a lo que se conoce como el suicidio digital: limitar el propio uso de productos o servicios proporcionados por determinadas compañías como una forma de resistencia a su poder. Fundamentalmente, esto consiste en dejar de utilizar las redes sociales y otros servicios de internet como las herramientas

de Google, o no utilizarlas como primera opción. Estas prácticas, cada vez más frecuentes, revierten en la práctica en una disminución de las exigencias a estas compañías por parte del usuario. Como explican Baruh y Popescu (2017), por una parte, con el abandono del producto o servicio por parte de estos usuarios críticos, se reducen las señales de las cuales disponen las empresas proveedoras de esos servicios para establecer sus políticas de privacidad. Por otra parte, dado que los consumidores que no están dispuestos a mercadear con su privacidad a cambio de beneficios dejan de utilizar estos servicios, el mercado genera la falsa asunción de que todos los usuarios conciben su privacidad de una forma pragmática.

La postura de Lanier (2018) es un ejemplo de este caso. En su libro *Ten Arguments For Deleting Your Social Media Accounts Right Now*, anima a sus lectores a eliminar sus perfiles de redes sociales. Defiende que esta es la forma más directa de resistir la insensatez y la desproporción de poder de los gigantes digitales. Es decir, "suicidarse digitalmente", en defensa propia.

Ofuscación

Otros, como Karppi (2011), argumentan que esto es únicamente una forma de intentar fútilmente ocultar la propia vida a la datificación. Al contrario, proponen que la respuesta más sensata es la ofuscación. Es decir, producir masivamente más datos de los que generarían las acciones humanas de forma "natural", como una táctica de disrupción. Dockray (31 de mayo de 2010) ha escrito uno de los textos más representativos de este movimiento. *The Facebook Suicide Bomb Manifesto* reivindica un suicidio social digital diferente. En él, Dockray alienta a generar una sobrecarga radical de información, capaz de "ahogar" el sistema en datos y así perturbar a los rastreadores, haciendo indistinguibles las expresiones reales de la actividad humana. En esta línea, Howe y Nissenbaum (2017: 1) han desarrollado *AdNauseam*, "an open-source browser extension that leverages obfuscation to frustrate tracking by online advertisers". Este software sigue un enfoque similar a uno desarrollado anteriormente, y llamado TrackMeNot: "a Firefox browser extension designed to achieve privacy in web search by obfuscating users' queries within a stream of programatically-generated decoys" (Howe y Nisseumbaum, 2009). Los desarrolladores explican la necesidad de esta herramienta en la página web de AdNauseam (2019) como consecuencia del

fracaso de la industria a la hora de auto-regular los excesos del rastreo en la red: "AdNauseam allows individual users to take matters into their own hands, fighting back against unilateral surveillance".

[OE5] La protección de los datos personales en Europa

Frente a esta explotación masiva, la Unión Europea reconoce la "protección de los datos personales" como un derecho fundamental. Así lo recogen el Tratado de Funcionamiento de la Unión Europea (2012/C 326/01), artículo 16.1: "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan." Y la Carta de Derechos Fundamentales de la Unión Europea (2016/C 202/2), artículo 8:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

Reglamento General de Protección de Datos

El 27 de abril de 2016 entró en vigor el Reglamento General de Protección de Datos del Parlamento Europeo y del Consejo (2016/679), fecha en que se derogó la anterior Directiva de Protección de Datos de 1995 (95/46/CE). El RGPD establece el marco jurídico para la protección de los datos personales en los estados miembros. Desde el 25 de mayo de 2018, es de cumplimiento obligatorio y directamente aplicable en todos los estados miembros de la Unión Europea. Dicho reglamento (artículo 1.1) "establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos."

En enero de 2016, cuando la entrada en vigor del RGPD era inminente, la Dirección General de Justicia y Consumidores de la Comisión Europea (2016) publicó en su web nueve informes a cargo de Vêra Jourová (la comisaria europea de Justicia, Consumidores e Igualdad de Género de la Comisión Europea), dedicados a resolver cuestiones clave acerca de la reforma de la legislación europea en materia de protección de datos. A lo largo de estos informes (véanse, por mayor relación con el tema de la

tesis: Jourová, Enero de 2016a; Enero de 2016b; Enero de 2016c; Enero de 2016d), se expone que el reglamento surge como respuesta a tres problemas principales derivados de la introducción de nuevas formas de comunicación, como las redes sociales, y al desarrollo tecnológico y la globalización, que permiten recopilar, transferir y utilizar datos de forma masiva y transnacional:

1. Aumenta la dificultad para proteger la privacidad de los datos.
2. Crece la desconfianza de los ciudadanos en el entorno digital.
3. Como consecuencia, el mercado interior y el Producto Interior Bruto de la UE de la UE se ven perjudicados.

Uno de estos informes, *La reforma de la protección de datos en la UE y los macrodatos* (Jourová, Enero de 2016b), se centra específicamente en las nuevas soluciones que aporta el RGPD en relación a los problemas de privacidad derivados de la explotación big data. Cabe destacar cómo el primer párrafo de dicho informe se centra en el valor económico de los datos masivos para las empresas de la UE:

> Según algunas estimaciones, el valor de los datos personales de los ciudadanos europeos podría llegar a alcanzar una cifra cercana al billón de euros anuales de aquí a 2020. Por tanto, el refuerzo de las estrictas normas europeas de protección de datos no supondrá un lastre para la innovación, sino un incentivo para la actividad económica. Los consumidores están cada vez más preocupados por su privacidad, y esta pérdida de confianza se traduce en una pérdida de oportunidades e ingresos para las empresas. Los recientes y sonados casos de violación de datos han llevado a los consumidores a huir de proveedores de servicios que no protegían adecuadamente sus datos personales. Las empresas de la UE que ofrecen servicios respetuosos de la privacidad pueden resultar más atractivas para los consumidores y, por tanto, más competitivas. La UE posee las normas de protección de datos más estrictas del mundo, y eso genera confianza.

A lo largo del documento, Jourová (Enero de 2016b: 4) insiste en la importancia económica de los datos masivos para el mercado interior europeo:

> La utilización de macrodatos por los cien principales fabricantes de la UE podría generar un ahorro de 425.000 millones EUR y, de aquí a 2020, el análisis de macrodatos podría aumentar el crecimiento económico de la UE en un 1,9 %, lo que supondría un incremento del PIB de 206.000 millones EUR.

En función de estos problemas, se repite a lo largo del conjunto de los informes (Jourová, Enero de 2016a; Enero de 2016b; Enero de 2016c; Enero de 2016d) que los principales propósitos del RGPD son tres:

1. resguardar el derecho fundamental a la protección de datos personales de los ciudadanos de la UE;
2. aumentar el nivel de confianza de los ciudadanos en el mercado digital,
3. y, gracias a ello, mejorar la "libre circulación de datos" entre los estados miembros, para aumentar la productividad de las empresas del mercado interior de la UE y su Producto Interior Bruto.

El objetivo de este apartado es exponer cómo se ha concretado el cumplimiento de estos objetivos en el RGPD.

De acuerdo con lo dispuesto en la Carta de Derechos Fundamentales de la UE, el RGPD establece el consentimiento individual "informado" como el principal mecanismo de que disponen los ciudadanos para "proteger" sus "datos personales". La expresión "datos personales" se define (artículo 4.1) como: "toda información sobre una persona física identificada o identificable («el interesado»)".

Por "persona física identificable", se entiende:

> toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

De acuerdo con los *Principios relativos al tratamiento*, establecidos en el artículo 5 del reglamento, los datos personales serán "tratados de manera lícita, leal y transparente en relación con el interesado". Además, "serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines". El principio de "minimización de datos" establece que los datos serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados", y también "exactos y, si fuera necesario, actualizados". Este mismo artículo establece que el cumplimiento de estos principios es responsabilidad de la persona o institución que trata los datos.

El artículo 4.2 define "tratamiento" como:

> cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o

> modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

Para que este tratamiento sea "lícito", debe cumplirse al menos una de las siguientes condiciones que recoge el artículo 6.1:

> a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
> b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
> c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
> d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
> e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
> f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero […]
> Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

El reglamento (artículo 9) prohibe el tratamiento de determinadas "categorías especiales de datos personales", que por su naturaleza se consideran particularmente "sensibles". En concreto:

> Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación [*sic*] sexuales de una persona física.

El artículo 9 añade que dicha prohibición no se aplica en los casos siguientes: la persona a la que se refieren los datos ha consentido ese tratamiento; si esta los ha hecho "manifiestamente públicos"; o si el tratamiento lo realiza "una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical" y dado el supuesto de que este tratamiento "se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines". Tampoco se aplica si el tratamiento es necesario para las siguientes cuestiones: dar cumplimiento a obligaciones legales; permitir el ejercicio de derechos específicos de alguna de las partes, relativas al derecho laboral, a la seguridad y a la protección social; proteger una vida, cuando la persona a la que se refieren los datos no puede dar su consentimiento; o

permitir el ejercicio de la justicia. O bien, si el tratamiento de los datos se realiza con fines: médicos o de "gestión de los sistemas de asistencia sanitaria y social"; de archivo, ya sean de interés público, de investigación científica o histórica, o con fines estadísticos; por razones de "interés público esencial", siempre que el tratamiento sea proporcional al objetivo perseguido; o por razones de "salud pública" y de "seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios".

Por "consentimiento del interesado" el RGPD entiende (artículo 4.11):

> toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

Dicho consentimiento debe ser previo a la recopilación o el uso de los datos. En el caso de que la licitud del tratamiento de los datos se base en el consentimiento de la persona a que se refieren, el responsable deberá ser capaz de demostrar que aquel consintió que lo hiciera (artículo 7.1).

Por otra parte, de acuerdo con los principios de lealtad, transparencia y "minimización de datos", el RGPD considera que el consentimiento individual no es libre si el individuo es forzado a ceder o aprobar el uso de determinados datos para la ejecución de un contrato o la prestación de un servicio, en el caso de que dichos datos sean innecesarios para tal contrato o servicio (artículo 7.4):

> Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

La persona, por tanto, consiente "libremente" si no está obligada a ceder más datos de los que se consideren proporcionados de acuerdo con la finalidad de su uso.

La responsabilidad de proporcionar la información necesaria para que el consentimiento sea "informado" la asume la parte interesada en la recopilación y/o el tratamiento de los datos. En el momento en que el responsable del tratamiento obtiene los datos, debe informar a la persona a la que estos datos se refieren sobre (artículo 13.1): la identidad y los datos del responsable del tratamiento; los fines del tratamiento; los intereses

legítimos del responsable o de un tercero en el tratamiento; los destinatarios o categorías de destinatarios de los datos; y la intención de transferir los datos a terceros.

Además, para garantizar que el tratamiento sea "leal y transparente" (artículo 13.2) el responsable del tratamiento debe proporcionar información sobre: el plazo durante el cual se conservarán los datos o el criterio mediante el cual se determinará ese plazo, los derechos de la persona a la que se refieren los datos respecto al tratamiento y la conservación de los datos; en los casos que proceda, el requisito legal por el cual la persona está obligada a facilitar los datos y las posibles consecuencias de no hacerlo; y la existencia de "decisiones automatizas, incluida la elaboración de perfiles", incluyendo en este caso información sobre la "lógica aplicada", así como la importancia y las "consecuencias previstas" de dicho tratamiento para el interesado.

A mayores, en el caso de que el responsable del tratamiento no haya obtenido los datos de la misma persona a la que se refieren esos datos (artículo 14.2.f), debe informarle de "la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público".

Además de conocer esta información, la persona a la que se refieren los datos tiene derecho: a solicitar acceso a los datos que le conciernen de los cuales dispone el responsable del tratamiento de forma fácil y "gratuita", a retirar su consentimiento ("sin que ello afecte al tratamiento basado en el consentimiento proporcionado antes de su retirada") y a presentar una reclamación ante una autoridad de control (artículo 14). Tiene también derecho a solicitar la rectificación (artículo 16), la supresión (artículo 17) o la portabilidad de los datos que le conciernen (artículo 20), o que se limite su tratamiento (artículo 18). Asimismo, puede oponerse al tratamiento (artículo 21) y a ser objeto de una decisión con efectos jurídicos o que le afecte significativamente de un modo similar y esté fundamentada de forma exclusiva en una forma automatizada de tratamiento de los datos (artículo 22).

También en este caso es la parte interesada en el tratamiento de los datos la responsable de dar cumplimiento a estos derechos. Está obligada a hacerlo si se dan determinadas condiciones, como que los datos ya no sean necesarios para los fines con los que se recogieron o que no prevalezcan motivos legítimos para el tratamiento. Pero no si el

tratamiento es necesario para ejercer el derecho a la libertad de expresión e información, para cumplir una obligación legal, por razones de interés público, investigación científica, o el ejercicio de la justicia, entre otras (véanse los artículos de 16 a 22).

En esencia

Atendiendo a lo expuesto en el apartado anterior, el objetivo de esta sección es perfilar cuál es la fundamentación teórica y conceptual del modelo de protección de datos personales en Europa. Su pretensión no es, por lo tanto, presentar un análisis exhaustivo del RGPD, sino comprender su sentido general. Posteriormente, esto permitirá analizar, en el apartado de Discusión, si el marco jurídico europeo de protección de datos personales se adecúa a los problemas derivados de la explotación de datos masivos [OG2–OE5].

El RGPD establece el marco jurídico para la "protección de las personas físicas en lo que respecta al tratamiento de datos personales". Pero ¿qué es exactamente aquello de lo que protege a las personas? Fundamentalmente, el RGPD establece que toda aquella información que se refiere a una persona identificable no pueda ser recogida o utilizada si esta persona no ha dado su consentimiento, o si su uso no está justificado por una causa legítima suficientemente justificada por el interés del afectado, el interés público o en el marco del ejercicio de una autoridad pública. Más allá de esto, dispone que los datos personales no pueden ser utilizados de forma desproporcionada respecto del fin para el que servirán, ni tampoco desleal o inadecuada.

En lo concreto, el principal mecanismo para el cumplimiento del derecho fundamental a la protección de datos personales es el consentimiento individual. Por ello, algunos autores (como Baruh y Popescu, 2017; Schwartz, 2013; o Solove, 2013) señalan que el modelo europeo se traduce en una forma de *autoprotección* que exige a la persona que identifique, comprenda y analice los perjuicios y los beneficios derivados de ceder unos determinados datos que se le requieren, en relación al fin concreto para el que se utilizarán. Y que, en función de esto, decida si consiente o no este uso. En este sentido, el marco europeo afianza una concepción de los datos personales como un bien "gestionable" (es decir, transferible o intercambiable) por otros de "valor" proporcional, que se debe proteger de ser "violado" de forma "injustificada".

Este modelo se conoce como el modelo de la "notificación y la elección" (traducido del inglés, *notice and choice*. Véase: Solove, 2013). O, más concretamente, de la notificación y el consentimiento. De forma similar, la regulación de protección de datos se restringe, en la práctica, a una forma de *autorregulación* del mercado, que, en cierto modo, se convierte en el garante del cumplimiento de los derechos de los ciudadanos.

De todo esto, se extrae que el modelo de protección de datos personales en Europa responde a lo que Baruh y Popescu (2017) denominan el paradigma de la "autogestión de la privacidad". En otras palabras, el marco de protección de datos personales toma sus bases de una concepción pragmática o utilitarista de otro derecho fundamental más amplio: el derecho a la privacidad.

En 1890, Warren y Brandeis definieron en su famoso texto *The Right to Privacy* la que todavía hoy muchos (como Richardson, 2016) reconocen como la concepción hegemónica del derecho a la privacidad en el mundo occidental: un derecho "contra el mundo", basado en los principios de "inviolabilidad de la personalidad" o "inmunidad da la persona". El objetivo de este derecho, según especificaron los autores, no es otro que proteger a las personas de los "perjuicios provocados" por la invasión injustificada de sus asuntos personales. En sus palabras (Warren y Brandeis, 1890: 7):

> The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, made public against their will. It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented.

Este derecho "ceases upon the publication of the facts by the individual, or with his consent" (Warren y Brandeis, 1890: 8). Los paralelismos con el modelo de protección de datos personales que establece el RGPD son claros.

Esta concepción negativa de la privacidad, como una esfera "inviolable" está fuertemente ligada al ideal liberal de libertad como *no-interferencia* (Berlin, 1969; Bobbio, 2009; Hobbes, 2011) o, en palabras de Warren y Brandeis (1890), al derecho más amplio a "ser dejado solo". Para el liberalismo, una persona es libre si puede decidir sobre cuestiones que afecten a sus libertades básicas sin que otros modifiquen esa decisión o le impongan deliberadamente las condiciones objetivas o cognitivas bajo

las cuales toma esa decisión. Por lo tanto, lo que va en contra de la libertad son todas aquellas interferencias activas y directas en la voluntad que guía el curso de acción de una persona. Uno es totalmente libre cuando hace lo que quiere hacer. Sin embargo, como es imposible que todos hagan lo que quieren, sin interferir a los otros en aquello que ellos quieren hacer, la libertad liberal debe ser limitada para permitir la vida en común y evitar conflictos entre la libertad individual y otros valores, como la seguridad o la propiedad. Esto tiene que ver con un relativismo moral que considera que es imposible otorgar importancia a los diferentes valores sociales de una forma objetiva, y que esto es, por el contrario, una cuestión puramente subjetiva, que corresponde en exclusiva a los individuos particulares. En este sentido, el estado debe ser lo más pasivo posible para interferir lo mínimo necesario en la libertad individual, y su papel debe restringirse a reducir las posibilidades de que unos fuercen a otros a tomar decisiones que puedan afectar a su vida de forma significativa.

Se sigue de este razonamiento que, si el estado liberal es especialmente pasivo en lo que respecta a la protección de lo personal o lo privado, al menos en teoría, lo hace con el objetivo de no interferir en las decisiones privadas. Por una parte, el componente "subjetivo" del valor de los asuntos privados parece más obvio que el de los asuntos "públicos". Por otra, el riesgo de que las decisiones individuales sobre la vida privada afecten a la vida privada de otro individuo, parece menor. Así, la "necesidad" del estado de restringir la libertad de uno de hacer lo que quiera en su espacio privado se limita a aquellos casos en los que un comportamiento privado pueda afectar de forma directa al bienestar o el interés públicos. Desde esta perspectiva, la privacidad es un refugio frente a las restricciones del estado liberal a la voluntad individual. Una esfera a prueba de interferencias del estado o de los demás y, por tanto, de libertad como no-interferencia en un sentido más "puro". Esto explica por qué la privada ha sido definida por el liberalismo como una esfera opuesta a la pública, y por qué lo personal y lo privado (como por ejemplo, los datos personales) se han considerado un asunto de auto-regulación (Mill, 1992).

No obstante, apunta Richardson (2016: 4), esta visión liberal-tradicional ha sido en cierto modo matizada por el tratamiento que han hecho de ella las posturas neoliberales, como un tipo de propiedad a la cual el mercado es extensible: "While liberal thought

dominates the canon, it is undermined by the neo-liberal images of the self as an entrepreneur, owner of one's own human capital." La autora, ha notado también que esta concepción pragmática de la privacidad, que manejan las legislaciones actuales, tiene mucho que ver con un fuerte interés por el creciente valor económico de los datos para el mercado, para el cual es esencial estabilizar la idea de los datos como una nueva "propiedad". A este respecto, destacan particularmente las alusiones explícitas y repetidas, recogidas en el apartado anterior, de las autoridades europeas al valor económico de los datos y a la importancia de generar entre los ciudadanos un clima de confianza en los entornos digitales, como una forma contribuir al PIB de la UE. Floridi (2013) ha hablado de los problemas de entender los datos como una propiedad, y apunta que nuestros datos son más bien parte de lo que "somos" que algo que nos "pertenece".

Crítica feminista a la privacidad

El feminismo ha dedicado gran parte de su teoría política a reflexionar sobre la forma en que el liberalismo ha concebido la dicotomía público/privado y sobre las consecuencias sociales de su puesta en práctica (Pateman, 1989). Este análisis ha llevado a muchas teóricas y teóricos del feminismo a denunciar un lado oscuro de la privacidad, que ha servido para ocultar y, en cierto sentido, para legitimar las causas objetivas de la subordinación de la mujer al hombre (MacKinnon, 1989). Desde esta perspectiva, el feminismo ha disputado de una forma especialmente destacable los límites de lo personal, lo privado, lo público y lo político (Agra Romero, 2012).

"Lo personal es político" es un lema ligado a las protestas del movimiento feminista radical de finales de 1960 a 1980, conocido como el "feminismo de segunda ola". Fue popularizado por dar título al manifiesto de Hanisch (1970) "The personal is political", publicado en *Notes from the Second Year*. El texto, que ha sido muy influyente en la teoría feminista posterior, subraya que, muchos de los problemas "personales" que sufren las mujeres en el ámbito privado o doméstico, no son sino un síntoma de su subordinación a los hombres en la estructura social. A este respecto cabe destacar el trabajo de Federici (2004), quien se ha centrado en explicar las causas históricas de la subordinación del hombre a la mujer, mediante una revisión de la división sexual del trabajo que impuso el capitalismo en sus orígenes.

El manifiesto denuncia que, precisamente porque la causa del problema no se encuentra en quien lo sufre (cada mujer), la lucha aislada es necesaria, pero no suficiente para resolver el problema, porque las situaciones opresivas hacen a la gente actuar "por necesidad" y no "por decisión". Así, reclama combatir el problema como un movimiento, para buscar las acciones y soluciones políticas necesarias.

El manifiesto, como explicó posteriormente Hanisch (2006), surgió en relación a unas sesiones de "terapia para mujeres" que formaban parte de las acciones del *Movimiento de Liberación de las Mujeres* ("Women's Liberation Movement"). Este representa la respuesta de Hanisch a las críticas recurrentes a la naturaleza política de esas sesiones de terapia y a una escisión del *movimiento* del cual ella que formaba parte. Esta escisión, fuertemente vinculada a la política radical socialista de la misma época, buscaba hacer parte de la discusión y la acción pública los "problemas personales" de las mujeres (incluyendo aquellos referidos al cuerpo, como el sexo, o el aborto) (Hanisch, 1970: 76): "Can you imagine what would happen if women, blacks, and workers […] would-stop blaming ourselves for our sad situations? It seems to me the whole country needs that kind of political therapy." Las críticas, explica Hanisch (2006: 1) estimaban inadecuado hacer político un problema personal: "if women would just "stand up for themselves" and take more responsibility for their own lives, they wouldn't need to have an independent movement for women's liberation".

Estos argumentos siguen siendo utilizados por lo que hoy Fraser (2017) denomina el "feminismo neoliberal", una de las expresiones de un "neoliberalismo progresista" imperante en el mundo occidental, que combina ideales enmancipadores con formas brutales de financierización de la economía. Un movimiento fuertemente ligado a los poderes del capitalismo global, que aprovecha esta tendencia individualista enmarcada en un momento de crisis para restar poder, poco a poco, a las formas de protección social.

Partiendo de la idea de "lo personal es político" una parte del feminismo (véanse: Fraser, 2012 o Millett, 1970) ha explicado que las relaciones de poder asimétricas (sean entre agentes públicos y privados, o exclusivamente entre agentes privados) dan inequívocamente lugar a la subordinación de la parte más débil. Asimismo, denuncia que, si las causas de esas desigualdades se dejan fuera de la discusión y de la acción

política, se pierden las opciones de resolver esos problemas como sociedad y de una forma democrática. En consecuencia, afirma Fraser (2012) se refuerza la tendencia liberal a "redefinir" las consecuencias de estas desigualdades de poder como "problemas personales": no hay más posibilidades de resolverlas que tomándolas como tales y combatiéndolas en el plano individual. Estas ideas, no sólo tienen un gran valor para la lucha de las mujeres, sino una relevancia a nivel teórico, que muestra algunas de las debilidades más importantes de la teoría liberal

Libertad republicana: control sobre el poder de interferencia

Ese lado oscuro de la privacidad que ha denunciado la teoría política feminista tiene mucho que ver con el hecho de entender la privacidad desde la idea liberal de libertad como *no-interferencia*.

El pensamiento político contemporáneo se divide entre quienes sostienen que la libertad consiste en la *no-interferencia* (liberales) y quienes defienden una concepción de la libertad como *no-dominación* (republicanos). Sin embargo, tanto desde la "izquierda" política, como desde la "derecha", la mayoría han asumido la no-interferencia como la forma natural de comprender la libertad (Pettit, 1996).

La libertad es un valor esencial. Dependiendo de cómo uno entienda la libertad variarán el sentido y el alcance de otros valores y también la forma de protegerlos. Esto es más evidente en el caso de ciertos valores, como la igualdad (ej: ser igualmente libres), pero quizás menos en el de otros, como la privacidad. La privacidad es, además, un valor que en la teoría política liberal ha tenido un papel central, pero al cual el republicanismo ha prestado poca atención (Roberts, 2015; 2018; van Der Sloot, 2018). Como consecuencia, es inusual para la academia, para la política y para el derecho pensar en la privacidad en términos diferentes a la no-interferencia. Sin embargo, como resultado del reciente repunte de la tradición republicana, algunos autores (como Gräf, 2017; Hoye y Monaghan, 2015; Newell, 2014; Roberts, 2015; 2018; o van Der Sloot, 2018) han planteado en los últimos años una necesidad de repensar los problemas derivados de las nuevas tecnologías de la vigilancia, en general, y el valor de la privacidad, en particular, desde la perspectiva de la no-dominación. Según Roberts (2018: 6): "re-examining the

beliefs that we hold about the nature of freedom —its constituent conditions— might, if it causes a shift in those beliefs, lead us to think differently about privacy".

Dada la importancia de esta cuestión para la presente tesis doctoral, las próximas páginas de este apartado se dedicarán a analizar las diferencias principales entre ambas teorías de libertad, a través de una explicación de la teoría republicana, dado que es la menos conocida de las dos.

El liberalismo y el republicanismo coinciden en que la libertad requiere que las personas puedan tomar decisiones libres en relación a sus libertades básicas (o derechos fundamentales). Además, ambas teorías definen la libertad en negativo (no-), como un derecho del individuo a que su vida y sus decisiones estén protegidas de alguna forma de invasión de la voluntad. Sin embargo, el liberalismo y el republicanismo difieren en dos cuestiones centrales: qué tipo de obstáculos pueden representar una invasión de la libertad de decisión y qué debe ser obstaculizado para que la libertad de una decisión se considere invadida (Pettit, 2012).

Para el liberalismo (Berlin, 1969), la libertad se considera invadida siempre que (y solo cuando) un obstáculo impida o frustre la posibilidad de que el individuo pueda conocer y elegir cualquiera de los posibles cursos de acción o las opciones posibles para una decisión, o que manipule, modifique o imponga dicho curso de acción o su elección final entre una y otra opción. En este sentido, el liberalismo equipara la invasión a la interferencia activa. Esto es lo que Pettit (2010: 38-39) denomina la "falacia liberal":

> The line of thought that I have been sketching shows that there are two ways in which the standard equation of freedom with noninterference goes wrong. First of all it makes the mistake of thinking that interference always mediates alien control and reduces freedom; it is guilty of what we might describe as the interference always fallacy. This mistake comes of a failure to recognize that interference may be controlled by the person interfered with, as when my partner hides the chocolate or cigars at my bidding, and that when it is nonarbitrary in that sense it does not mediate the alien control of another and does not reduce my freedom.
>
> The second mistake in the standard approach may be described, in parallel, as the interference-only fallacy. This consists in the thought that only interference can mediate the alien control of another and so only interference can have the effect of reducing freedom. This thought is mistaken because, as we have seen, others may impose their wíll on me, exercising an alien control, just by resort to invigilation or intimidation; they need not interfere in order to reduce my freedom.

El republicanismo actual, o neorrepublicanismo es una filosofía política sobre la libertad y el gobierno. En las próximas líneas se explican sus ideas a través de las aportaciones de Philip Pettit[4] (1996; 1997; 2010; 2012).

Pettit (2010) utiliza el adjetivo "cívica" para diferenciar su teoría de otras tres acepciones comunes del *republicanismo*:

- el republicanismo como mera oposición a la monarquía;
- el republicanismo del Partido Republicano estadounidense;
- y el republicanismo referido por la filosofía *comunitarista*, basado en una concepción "positiva" de la libertad individual, que se equipara, en sí misma, a la participación política.

El republicanismo, se aleja de esta última concepción positiva de la libertad para defender una negativa, que no aporta la participación política en sí misma, sino los frutos que se extraen de esa participación. Pettit defiende que una visión positiva de la libertad falla al dar por hecho que todos tienen las mismas posibilidades, capacidades y oportunidades de participar en la política. Por el contrario, el republicanismo se ocupa de la libertad individual en tanto que un bien cívico, social o político (Pettit, 2012: 49) —la *no-dominación*— que la participación política ayuda a alcanzar:

> Our concern is solely with social free will or, in effect, political freedom: that is, with what is required for it to be the case that however imperfectly formed your will may be, you are in a position to make your choice, without vitiation or invasion, according to that will.

Dominación: un poder de interferencia incontrolada

Ser *dominado* significa estar expuesto a un "poder de interferencia incontrolada" —o de "interferencia arbitraria", en trabajos anteriores de Pettit (1997)—. Un agente o una agencia, *X* (que puede ser individual o colectivo) domina a otro, *Y* (a menudo individual), si *X* dispone de un poder para interferir (si así lo desea) en la vida o las decisiones de *Y*, que *Y* no controla por sí mismo. Esto sigue siendo válido en el caso de que *X* no desee disponer de ese poder, aunque nunca vaya a hacerlo efectivo para

[4] Pese a que numerosos autores y autoras han teorizado en los últimos años sobre la teoría republicana, Philip Pettit es ampliamente considerado el filósofo más relevante del neorrepublicanismo. Sus dos obras más importantes son: *Republicanism: A Theory of Freedom and Government* (1997) y *On the People's Terms: A Republican Theory and Model of Democracy* (2012).

interferir activamente en la vida o las decisiones de *Y*, y aunque *Y* no sea consciente de su vulnerabilidad ante *X*. Así, la dominación, no requiere ni que *X* ejerza una interferencia activa sobre *Y*, ni que desee hacerlo, ni que lo vaya a hacer en el futuro. Por contraste, la dominación es inherente a la capacidad de *X* de hacerlo sin que *Y* pueda controlarlo. El motivo es que, dada esta capacidad de *X*, la vida o las decisiones de *Y* quedan (en alguna medida) subordinadas a la voluntad de *X*, independientemente de si la voluntad de *X* es utilizar ese poder del que dispone, o no hacerlo.

De esto se extrae que la dominación a la que se refiere Pettit tiene una naturaleza disposicional, como la fragilidad o la elasticidad, que puede o no tener una manifestación contingente. Esto marca una clara diferencia con la teoría liberal. Decidir libremente, en sentido republicano, no sólo quiere decir que la decisión no sea impuesta, modificada o frustrada por otro, sino que esa decisión no esté influida (directa o indirectamente) por una voluntad o un interés ajeno sobre el que uno mismo no tiene capacidad de control.

Por eso, de acuerdo con Pettit (2012), una decisión solo es libre si quien la toma tiene la capacidad de utilizar los recursos personales, naturales y sociales (materiales e inmateriales) necesarios para elegir entre el abanico de todas las posibles opciones de esa decisión (independientemente de cuál sea la preferida) de acuerdo con la propia voluntad y sin depender de nadie para hacerlo. Pero, para percibir como posibles todas esas opciones y poder utilizar dichos recursos para elegir entre ellas de acuerdo con la propia voluntad es necesario, antes, poder acceder objetiva y cognitivamente a esas opciones y a esos recursos. Ser libre para decidir "is to exercise the capacity that the resources put in your possession in order to satisfy your will or preference over the options" (Pettit, 2012: 36).

Obstáculos viciantes e invasivos

En este sentido y de forma opuesta al liberalismo, que en ningún caso lo contempla, tanto la libertad como la dominación están directamente relacionadas con la "capacidad" o el "poder". Domina quien tiene un poder que le permitiría interferir en la vida del dominado, si este último no tiene el poder de controlar esa interferencia. Y es libre quien tiene el poder para acceder objetiva y cognitivamente a una serie de recursos

y utilizarlos como quiera, sin depender de nadie para hacerlo. Como consecuencia, el republicanismo reconoce dos tipos de obstáculos capaces de limitar la libre decisión: los *viciantes* y los *invasivos* (Pettit, 2012):

Los obstáculos viciantes son aquellos que dificultan o impiden la capacidad de uno para acceder a esos recursos y de usarlos en general. También si este impedimento general implica no poder usarlos para satisfacer la propia voluntad. Estos obstáculos los provocan factores que no controla ni uno mismo, ni los demás (Pettit, 2012: 39):

> Such failures of resources may derive at any time from your own illness or disability, from the limits of your natural environment, from the continuing, damaging results on you or your environment of the invasion of earlier choices, from the aggregate consequences of independently motivated actions by others, or from the actions of another agent that are necessitated in some way and not a matter of voluntary choice […]

Los obstáculos invasivos son aquellos que influyen en la capacidad de uno para usar esos recursos para el propósito específico de satisfacer la propia voluntad. En tanto que se refieren al propósito específico de satisfacer la propia voluntad, los obstáculos invasivos dependen necesariamente de una voluntad ajena (Pettit, 2012: 39):

> […] subjection to the will of another, be it total or partial, represents one way in which your choice may be invaded, being subject to a specific rather than a generic hindrance. But such subjection to another agent's or agency's will also looks to be the only way in which a choice may be invaded.

Cada uno de estos dos tipos de obstáculos afectan a dos dimensiones diferentes de la libertad de decisión. Por una parte, los viciantes impiden de forma genérica acceder o usar los recursos necesarios para una decisión. Es decir, limitan una precondición para la libertad de decisión. Pettit (2012: 45) se refiere a esta dimensión como la "libertad de oportunidad". Por otra parte, los invasivos, limitan la capacidad de usar esos recursos de acuerdo con la propia voluntad. Es decir, de ejercer control sobre la propia vida y decisiones y sobre la capacidad de otros de interferirlas. A esta otra dimensión la denomina "libertad de ejercer control".

En tanto que ser libre implica poder controlar la capacidad de otros para interferir en la propia vida, solo los obstáculos invasivos son, en sí mismos, constitutivos de dominación. No obstante, recalca Pettit (2012), sin libertad de oportunidad, la libertad de control se ve perjudicada. Por ello, aunque los obstáculos viciantes no representen en

sí mismos una forma de dominación, no se les debe restar importancia. En tanto que limitan el rango de opciones posibles y el acceso y el uso de recursos necesarios para la decisión, los obstáculos viciantes exponen a quien los sufre a un mayor grado de invasión por parte de otros.

Interferencia, vigilancia e intimidación

Centrándonos ahora en los obstáculos invasivos, hay diferentes formas mediante las cuales un agente o agencia puede ejercer dominación sobre otro. Aquí radica otra de las diferencias fundamentales con el liberalismo: para el republicanismo, la *interferencia activa* es solo una de las tres posibles formas de hacerlo. Las otras dos son la *vigilancia* y la *intimidación*:

Pettit (2012: 49) define la *interferencia activa* como el acto de intervenir intencionada y activamente en la decisión de otro para impedirla, restringirla o cambiarla. La interferencia se puede ejercer eliminando opciones, reemplazándolas o infrarrepresentando unas con respecto a otras, tanto objetivamente, como cognitivamente (en este útimo caso, para que el agente interferido no las perciba como posibles). En este sentido, y de nuevo a diferencia del liberalismo, la interferencia no se considera en sí misma contraria a la libertad, dado que un agente puede interferir en las decisiones de otro de un modo que este último controla. Con ello, si la interferencia activa se realiza de acuerdo con la voluntad y en los términos del agente interferido, no comporta dominación. En este punto, Pettit destaca la importancia de que, para que una interferencia no represente dominación, esta debe atender a la voluntad (a la voluntad revelada) del agente interferido, y no a sus "intereses". Es una precisión relevante, dado que elimina del mapa de lo posible aquel tipo de interferencias paternalistas y despóticas, realizadas por y para el interferido, pero sin su voluntad.

Pero, Pettit recalca que hay otras formas de invadir una decisión sin interferir de ninguna manera con el agente dominado, simplemente por el hecho de disponer de un poder incontrolado para hacerlo. Tanto la vigilancia como la intimidación representan esta forma de invasión:

La *vigilancia* (*invigilation*) tiene, en la obra de Pettit (2012), un sentido parecido a lo que también se podría llamar "monitorización" o "supervisión". Un ejemplo sería la

"vigilancia" que ejerce el profesor o la profesora que, durante un examen, observa la conducta de sus alumnos, sin ningún propósito de interferir en ella, a no ser que alguno se desvíe de lo que esta considere "adecuado". Siguiendo la explicación de Pettit, mediante la vigilancia, un agente observa lo que hace otro y, al hacerlo, adquiere la capacidad objetiva de interferir en su vida. No obstante, no lo hace, bien porque no es lo que desea, o bien porque no encuentra motivos para hacerlo. Dado que en esta forma de dominación, el vigilante no interfiere con el vigilado, las decisiones de este último, reflejarán su propia voluntad, pero únicamente y de forma subsidiaria porque no ha sido la voluntad del vigilante utilizar su poder para interferir en ella. Es decir, que, de igual modo, la voluntad del vigilado está subordinada a la del vigilante.

En el caso de que el vigilado se dé cuenta de que está siendo vigilado, entonces la capacidad del vigilante para eliminar, reemplazar o infrarrepresentar alguna de las opciones ya no solo es objetiva, sino también cognitiva. En este caso, el tipo de invasión de la voluntad a que se enfrenta el vigilado es denominada por Pettit *intimidación*. Pero, de hecho, la parte dominante también puede ejercer intimidación sin vigilar al agente dominado, simplemente haciéndole creer que dispone del poder para interferir en su vida. De nuevo, la voluntad del agente intimidado pasa a estar subordinada a la del intimidante.

A modo de resumen, un agente puede intervenir directamente en la vida de otro (interferencia activa), o puede situarse en una posición desde la cual podría interferir si esa es su voluntad (vigilancia), o puede hacer ver que está en esa posición desde la cual podría interferir (intimidación). Y todas ellas constituyen una forma de dominación en el caso de que el agente afectado no las pueda controlar.

Control vs. consentimiento

La teoría republicana (Pettit, 1997; 2010; 2012) explica que la dominación ejercida por *X* no tiene por qué dar lugar a una variación de la decisión de *Y* entre dos opciones diferentes, como "*sí*" y "*no*". Más bien, resulta en una transformación de la decisión "*sí*" por una del tipo: "*sí* (porque *X* quiere que sea *sí*)", o "*sí* (porque *X* no quiere que sea *no*)", o "*sí* (porque *X* no quiere influir en la decisión de *Y*)". O podría modificarla, transformando "*sí*" por: "*no* (porque *X* no quiere que sea *sí*)", o por "*no* porque *X* no

quiere que *Y* decida en base a su voluntad", etc. Es decir, en sentido republicano, la dominación (disponer de un poder que permite limitar la libertad) y la defensa de la libertad (controlar a quien puede limitar la libertad), más que una cuestión de *ausencia de interferencia*, son una cuestión de *control*.

Según la teoría de Pettit, tener control sobre algo implica dos cuestiones esenciales: tener cierta influencia sobre el proceso por el que ese algo se produce y poder usar esa influencia para modificar la dirección del proceso. Pettit (2012: 156), reconoce tres tipos de *influencia*, que ilustra con el siguiente ejemplo:

> Think of how I may control a horse that I ride. I may actively pull on the reins, now steering the horse in this direction, now in that. Or I may let the horse follow its head, given that it is moving in the direction I want to take. Or I may let the horse have free rein, given that I am happy for it to go wherever it wishes.

El primer tipo es la *influencia activa*: *X* interviene (interfiere activamente) para modificar o frustrar la decisión de *Y*. El segundo tipo es la *influencia virtual*: *X* no frustra la decisión de *Y*, porque esta decisión le satisface, pero lo haría si esta decisión cambia o deja de satisfacerle. En este caso *X* ejerce sobre *Y* una forma de interferencia que no da lugar a frustración. El tercer tipo es la *influencia reservada*: *X* se mantiene igualmente en una posición desde la cual puede interferir en el curso de acción de *Y*, pero no interfiere porque actualmente no es su voluntad hacerlo. Sólo si la voluntad de *X* cambia, esta forma de influencia daría lugar a una interferencia en la decisión de *Y*. Es el tipo de influencia que se ejerce mediante la vigilancia.

Si *X* dispone del poder de interferir en la vida de *Y*, pero *Y* puede controlar ese poder del que dispone *X*, entonces el poder de interferencia de *X* no domina a *Y*. Esto marca otra de las diferencias fundamentales de la teoría republicana con respecto a la liberal: *controlar* un poder de interferencia es bastante diferente a *consentir* o *desaprobar* una determinada interferencia. Por una parte, es posible consentir una interferencia sobre la que no se tiene control. Por otra, es posible controlar una interferencia sin necesidad de consentirla.

Esta, explica Pettit (2012), es la razón por la cual el republicanismo no considera el consentimiento como una forma de libre decisión y, por tanto, de protección de frente a la dominación.

Dominación vertical, horizontal y estructural

La dominación, como ha sido caracterizada hasta el momento, puede ser ejercida tanto por otros agentes o agencias privados, como por otros agentes o agencias públicos. En el caso de la dominación que proviene de los poderes privados, o dominación *horizontal*, Pettit (2010: 34) utiliza el término "*dominium*". Por otra parte, "*imperium*" se refiere a la dominación *vertical*, o de los poderes públicos (incluyendo el estado en sí mismo). La principal diferencia entre ambas es la siguiente: mientras que, en una sociedad democrática se espera que existan mecanismos de control ciudadano frente al *imperium*, esto no ocurre frente al *dominium*.

Pettit (2012) reconoce, además, que la misma forma cultural, económica o jurídica en que se organiza una sociedad puede dar lugar a una tercera forma de *dominación estructural*. La organización social, explica, configura un patrón en el que las diferencias de poder entre unos y otros, sitúan a los más poderosos en una posición de dominación (aun en el caso de que estos no deseen tenerlo, o utilizarlo). Pero, subraya (2012: 44), dicha organización no tiene por qué ser únicamente el resultado de las acciones de aquellos que se benefician de ella: "it may be the unintended, aggregate consequence of how people are independently motivated to act". En ese sentido, explica Pettit (2012: 63): "These modes of organization may vitiate, but not invade, choice, as when they emerge for example from customary practice, but they can indirectly facilitate the worst forms of invasion and domination in a society."

La dominación estructural puede no ser el resultado de una determinada voluntad y, por lo tanto, no representar una invasión de la libertad de otros. No obstante, sus efectos son tan similares a una forma de invasión de la libertad, que en la teoría de Pettit es considerada también una forma de dominación.

Justicia social, control popular y distribución de recursos

Todo lo expuesto en este apartado pone de manifiesto un componente social de la libertad republicana. Con ello, supera el individualismo inherente a la libertad liberal: mientras la libertad liberal no admite las interferencias ajenas, la libertad republicana no admite la subordinación de unos a otros. Si es posible que uno tenga la capacidad de exponer a otro a su poder de interferencia, aunque posteriormente se le impida interferir,

no es la libertad de ninguno de los dos lo que se protege. Al reconocer esta importancia del elemento de poder para la libertad, el republicanismo (Pettit, 2012) entiende la libertad sobre la base de la igualdad entre los ciudadanos y, por tanto, como un bien directamente relacionado con la justicia social. La teoría republicana de justicia social, explica Pettit (2012: 63-64) busca combatir las formas horizontales y estructurales de dominación, "looking for measures whereby people can be assured on a public basis of not being dominated by others in the broad range of the basic liberties".

En esta línea, explica Pettit, la dominación requiere ser contenida, no sólo mediante el control del individuo que la sufre, sino también por procesos de control externo a la relación de dominación, capaces de eliminar, reemplazar o infrarrepresentar la posibilidad de unos de dominar a otros. Pettit atribuye este poder de contención al ejercicio de los poderes democráticos del estado[5]. Para que todos sean libres, los poderes democráticos deben promover que las decisiones de unos sean, además de no-viciadas y no-dominadas, *co-ejercitables* y *co-satisfactorias* (Pettit, 2012: 93). No obstante, para que estos poderes públicos no ejerzan, a su vez, una dominación vertical, su ejercicio debe estar sometido al control popular. Este control popular es lo que Pettit (2012: 146) llama *political legitimacy* ("legitimación política"). Implica que los ciudadanos deben poder influir (tener una capacidad no viciada y no invadida para supervisar e intervenir) en estas formas de control externo y deben poder utilizar esa influencia para imponer una dirección determinada sobre el mismo. Para que todo esto sea posible, es además fundamental que los poderes públicos asuman la responsabilidad de redistribuir los recursos de una forma justa, de modo que la falta de recursos de unos no les impida controlar a otros con más recursos y el poder para influir en sus libertades básicas (Pettit, 2012).

[5] Antes de acabar este apartado, vale la pena apuntar dos críticas a la teoría de Pettit que se derivan de las aportaciones de otros autores afines a la teoría republicana (véanse: Bohman, 2007; Hoye y Monaghan, 2015; Martí, 2015; Martí y Seleme, 2015; y, desde una perspectiva diferente: Bellamy, 2019). Pese a que no se profundizará más en ellas, son de interés para el tema de esta tesis y, probablemente, serán una vía de trabajo en futuras investigaciones. En resumen serían las siguientes: La primera argumenta que la distinción de Pettit entre la dominación *horizontal* y la *vertical* no se produce en la práctica, ni define con precisión la realidad de un mundo globalizado, en el cual los diferentes poderes estatales (sean o no democráticos) pueden ejercer presiones más allá de sus fronteras, que no son controlables por los ciudadanos. Un ejemplo de ello es el creciente poder de países como China. La segunda, fuertemente ligada a esta primera, replica la tesis de que el contrapoder democrático frente a la dominación debe ser esencialmente estatal. La idea es que, en un mundo globalizado, donde los principales poderes privados son corporaciones multinacionales, y en el cual la soberanía de los estados es desigual, la contención democrática frente a la dominación debe ser, igualmente, transfronteriza.

Publicaciones del compendio

Lista de publicaciones

1. Suárez-Gonzalo, Sara y Guerrero-Solé, Frederic (2016). La conversación sobre big data en Twitter. Una primera aproximación al análisis del discurso dominante, *Comunicació. Revista de recerca i d'anàlisi*, *33*(2): 113-131. doi: 10.2436/20.3008.01.151. Disponible en: http://revistes.iec.cat/index.php/TC/article/view/142259/141168. [6]

2. Suárez-Gonzalo, Sara; Mas-Manchón, Lluís y Guerrero-Solé, Frederic (2019). Tay is you. The attribution of responsibility in the algorithmic culture, *Observatorio (OBS*), 13*(2): 1-14. doi: https://doi.org/10.15847/obsOBS13220191432. [7]

3. Suárez-Gonzalo, Sara (2017). Big social data: límites del modelo *notice and choice* para la protección de la privacidad, *El profesional de la información, 26*(2): 283-292. doi: https://doi.org/10.3145/epi.2017.mar.15. [8]

4. Suárez-Gonzalo, Sara (2018). Your likes, your vote? Big personal data exploitation and media manipulation in the US presidential election campaign of Donald Trump in 2016, *Quaderns del CAC, XXI*(44): 25-33. Disponible en: https://www.cac.cat/sites/default/files/2019-01/Q44_Suarez_EN_1.pdf. [9]

5. Suárez-Gonzalo, Sara [*en edición*]. Personal data are political. A feminist view on privacy and big data, *Recerca. Revista de pensament i anàlisi*. [10]

---

[6] Artículo indexado en la colección principal de Web of Science. Revista indexada en Web of Science Core Collection - Emerging Sources Citation Index. También en repositorios como CARHUS Plus+ 2014, FECYT o MIAR.

[7] Revista indexada en SCOPUS, Q3 (entre otras).

[8] Revista indexada, entre otros, en la colección principal de Web of Science, Q1 y SCOPUS, Q1. InCites Journal Citations Report: Journal Impact Factor 2017 = 1.318.

[9] Revista indexada en CARHUS Plus+ 2014.

Este artículo también se ha publicado en castellano y en catalán:

- Suárez-Gonzalo, Sara (2018). Tus *likes* ¿tu voto? Explotación masiva de datos personales y manipulación informativa en la campaña electoral de Donald Trump a la presidencia de EEUU 2016, *Quaderns del CAC, XXI*(44): 25-33. Disponible en: https://www.cac.cat/sites/default/files/2019-01/Q44_Suarez_ES.pdf.
- Suárez-Gonzalo, Sara (2018). Els teus *likes*, el teu vot? Explotació massiva de dades personals i manipulació informativa en la campanya electoral de Donald Trump a la presidència dels EUA 2016, *Quaderns del CAC, XXI*(44): 25-33. Disponible a: https://www.cac.cat/sites/default/files/2019-01/Q44_Suarez_CA.pdf.

[10] Los artículos de esta revista están indexados en la colección principal de Web of Science. Revista indexada en Web of Science Core Collection - Emerging Sources Citation Index y SCOPUS, Q2 (entre otras).

1

Suárez-Gonzalo, Sara y Guerrero-Solé, Frederic (2016). La conversación sobre big data en Twitter. Una primera aproximación al análisis del discurso dominante, *Comunicació. Revista de recerca i d'anàlisi*, *33*(2): 113-131. doi: 10.2436/20.3008.01.151.

Disponible en: http://revistes.iec.cat/index.php/TC/article/view/142259/141168.

ISSN: 2014-0304. ISSN electrónico: 2014-0444.

Comunicació: Revista de Recerca i d'Anàlisi [Societat Catalana de Comunicació]
http://revistes.iec.cat/index.php/TC. Vol. 33 (2) (novembre 2016), p. 113-131
ISSN (ed. impresa): 2014-0304 / ISSN (ed. electrònica): 2014-0444 / DOI: 10.2436/20.3008.01.151
Data recepció: 16/11/15
Data acceptació: 09/12/15

La conversación sobre *big data* en Twitter. Una primera aproximación al análisis del discurso dominante

La conversa sobre big data *a Twitter. Una primera aproximació a l'anàlisi del discurs dominant*

The conversation about big data on Twitter. An approach to the analysis of the dominant discourse

Sara Suárez-Gonzalo[1]
Estudiant del doctorat en comunicació del Departament de Comunicació de la Universitat Pompeu Fabra, Barcelona
sarapaz.suarez01@estudiant.upf.edu

Frederic Guerrero-Solé
Investigador i professor lector del Departament de Comunicació de la Universitat Pompeu Fabra, Barcelona
frederic.guerrero@upf.edu

SARA SUÁREZ-GONZALO I FREDERIC GUERRERO-SOLÉ

La conversación sobre *big data* en Twitter. Una primera aproximación al análisis del discurso dominante

La conversa sobre big data *a Twitter. Una primera aproximació a l'anàlisi del discurs dominant*

The conversation about big data on Twitter. An approach to the analysis of the dominant discourse

RESUMEN:
El análisis de grandes cantidades de datos (*big data*) se vislumbra como el nuevo paradigma de acceso al conocimiento en campos tan diversos de la ciencia como la medicina, la biología, la física o las ciencias sociales. El procesamiento de los datos obtenidos de buscadores y redes sociales se ha convertido en una pieza esencial para la definición de estrategias en política, economía o *marketing*. Este trabajo analiza la presencia de informaciones sobre *big data* en una de las principales redes sociales, Twitter. Sus objetivos son la jerarquización de usuarios y mensajes en función de su influencia en la conversación sobre *big data*, así como la identificación de los temas dominantes en la red, a partir del análisis del contenido de los mensajes analizados. Los resultados indican una clara orientación de la información sobre *big data* hacia los negocios, la predicción y la toma de decisiones.

PALABRAS CLAVE:
***big data*, predicción, redes sociales, Twitter, influencia, análisis de contenido.**

La conversa sobre *big data* a Twitter. Una primera aproximació a l'anàlisi del discurs dominant

La conversación sobre big data *en Twitter. Una primera aproximación al análisis del discurso dominante*

The conversation about big data on Twitter. An approach to the analysis of the dominant discourse

RESUM:
L'anàlisi de grans quantitats de dades (*big data*) s'albira com el nou paradigma d'accés al coneixement en camps tan diversos de la ciència com la medicina, la biologia, la física o les ciències socials. El processament de les dades obtingudes de cercadors i xarxes socials s'ha convertit en una peça essencial per a la definició d'estratègies en política, economia o màrqueting. Aquest treball analitza la presència d'informacions sobre *big data* en una de les principals xarxes socials, Twitter. Els seus objectius són la jerarquització d'usuaris i missatges en funció de la seva influència en la conversa sobre *big data*, així com la identificació dels temes dominants a la xarxa, a partir de l'anàlisi del contingut dels missatges analitzats. Els resultats indiquen una clara orientació de la informació sobre *big data* cap als negocis, la predicció i la presa de decisions.

PARAULES CLAU:
***big data*, predicció, xarxes socials, Twitter, influència, analisi de contingut.**

The conversation about big data on Twitter. An approach to the analysis of the dominant discourse

La conversación sobre big data *en Twitter. Una primera aproximación al análisis del discurso dominante*

La conversa sobre big data *a Twitter. Una primera aproximació a l'anàlisi del discurs dominant*

ABSTRACT:
Big data analysis is emerging as the new paradigm of access to knowledge in such diverse fields of science as physics, medicine, genetics, social sciences, economy and communication. The analysis of data collected from social networks or search engines has become essential to know how humans communicate, as well as to define strategies in politics, economics or marketing. This paper analyses the presence of information about big data in one of today's major social networks, the microblogging site Twitter. The main objective of this paper is the classification of users and posts in terms of their influence on the conversation about big data, and the identification of the dominant discourse in Twitter by analyzing the content of the messages posted. Our results point out a clear orientation of the information about big data towards business, prediction and decision making.

KEYWORDS:
big data, prediction, social networks, Twitter, influence, content analysis.

1. Introducción

Big data se ha convertido en uno de los principales focos de análisis en el entorno académico e investigador, y en uno de los principales sectores de inversión de muchas compañías y administraciones que ven en el tratamiento de grandes cantidades de datos (conjuntos de más de 1 terabyte) una forma de mejorar rendimientos y tomas de decisión o de realizar predicciones de futuro. Las razones de la aparición de este fenómeno son, sin duda, variadas y complejas, y se vinculan a un fuerte cambio en el contexto sociotecnológico que tiene su origen a principios del siglo XXI. Minelli, Chambers y Dhiraj (2013) aluden a la concurrencia de lo que llaman «tres tormentas perfectas»: la de la computación, la de los datos y la de la convergencia, que han tenido una enorme repercusión en la economía global. El actual desarrollo e implementación de herramientas diseñadas para la recolección, agregación, análisis, gestión y visualización de grandes cantidades de datos es creciente. Estas se diseñan con el objetivo de extraer de masas informes de datos información sobre cuestiones concretas, comprender las relaciones existentes entre los datos y vislumbrar patrones de comportamientos que hasta ahora permanecían ocultos (Boyd y Crawford, 2012; Shroek, Shockley, Smart, Romero-Morales y Tufano, 2012). Se espera que la analítica predictiva contribuya a anticipar algunas de estas conductas y también actuaciones y respuestas específicas de las personas, en función de probabilidades basadas en datos de situaciones similares anteriores, lo que podría tener una enorme repercusión en la producción, la logística o la estrategia de ventas de las empresas (Mayer Schönberger y Cukier, 2013: 151).

2. *Big data*, un término ubicuo de significado difuso

Nuestro estudio parte de una cuestión crítica: el término *big data* carece de una definición clara, única y consistente. Para comprender esta problemática y su importancia la contextualizaremos brevemente a continuación.

El término *big data* sienta sus bases en el año 1997 a manos de dos investigadores de la NASA para hacer referencia a un nuevo problema de magnitud. En este momento, *big data* da nombre a aquellas cantidades de datos lo bastante grandes como para no poder ser almacenadas en la memoria principal, el disco local o cualquier otro disco remoto de los ordenadores del momento (Cox y Ellswozrth, 1997: 1). En 2001, Laney (2001: 1) propone las tres V que definirán esta nueva forma de generación de datos (*velocidad*, *volumen* y *variedad*), a la que posteriormente y desde el sector empresarial se añade una cuarta, la *veracidad*. Más de una década después de su aparición, en 2011, el término comienza a popularizarse y su interés va en aumento de forma exponencial en el sector público y mediático. A partir de entonces, diferentes actores individuales o colectivos afectados por este nuevo

contexto o con intereses de diferentes índoles sobre él, plantean diversas definiciones del término. A esto se suma su naturaleza compleja, en la que se entrelazan una gran diversidad de aspectos técnicos y sociotecnológicos, así como aportaciones desde campos de conocimiento muy dispares. Por otra parte, el epíteto *big* conlleva una complicación añadida: connota importancia, complejidad y desafío, pero también se refiere a una cuestión de magnitud (que, como hemos visto, es esencial en su origen) (Ward y Barker, 2013).

Desde el nacimiento del término *big data* y su posterior popularización, se ha avanzado enormemente en el desarrollo e implementación de las tecnologías necesarias para el almacenamiento y el análisis de datos, y se ha superado así el problema de magnitud al que entonces hacía referencia. De este modo, el significado inicial del término pierde parte de su sentido. Dichos avances tecnológicos tienen una gran repercusión en diversos sectores de actividad, lo que aumenta las potencialidades de *big data* y lo vincula con diferentes realidades. Encontramos ejemplos de referencia en los sectores del transporte (UPS), infraestructuras (General Electric), venta por Internet (Amazon), seguros de salud (United HealthCare) o servicios financieros (Citigroup) (Davenport, 2014). Esto problematiza todavía más la existencia de una definición única. En este sentido, autoras como Boyd y Crawford (2011: 1) o Galdón (2014) han hablado de la *pobreza* del término *big data* (precisamente por esta alusión tan fuerte a una cuestión de magnitud) y sostienen que debería reinventarse para hacer eco de su complejidad real.

En la actualidad, unos autores conciben *big data* como un nuevo *data ecosystem*, cuya principal característica es la alta conectividad entre los datos, independientemente de su formato, su contenido y su fuente de procedencia, y que permite la obtención de información tan valiosa como el reconocimiento de patrones (Boyd y Crawford, 2011; Galdón, 2014; Minelli *et al*., 2013). Otros lo entienden como una mecánica de recolección y almacenamiento de datos (Baruh y Popescu, 2015: 3), de la que extraer nuevas formas de valor para los mercados, las empresas e instituciones públicas como los gobiernos (Mayer-Schönberger y Cukier, 2013: 6), y donde la usabilidad de los mismos adquiere una importancia central (Minelli *et. al*., 2013: 5). Hay incluso quien lo define como «a process to deliver decision-making insights» (Kalyvas y Oberly, 2014: 1). Además, estos vinculan a *big data* diferentes tecnologías, como la inteligencia artificial o el *Machine Learning*, y técnicas como la analítica de datos masivos. Esta visión, más utilitarista, se ha plasmado en algunas de las definiciones de mayor relevancia, provenientes de organizaciones como Gartner, Intel, Microsoft u Oracle (Ward y Barker, 2013).

Por otra parte, hay que señalar que el debate sobre las posibilidades del análisis de grandes cantidades de datos está polarizado entre dos grupos. Uno, el de aquellos que consideran *big data* como la nueva revolución que permitirá la mejora de muchos aspectos de nuestras vidas (entre ellos, la posibilidad de curar enfermedades o de proponer tratamientos a medida, e identificar factores y hábitos de riesgo) y lo ven como el final definitivo de la teoría y el inicio de una nueva era gobernada

por los datos (Mayer-Schönberger y Cukier, 2013; Davenport, 2014). Otro, el de aquellos que se muestran escépticos respecto a las cuestiones que puede resolver (Boyd y Crawford, 2012; Etlinger, 2014), y también el de los que ven en él un futuro distópico controlado por los datos, en el que se impondrá una nueva lógica de la vigilancia (Baruh y Popescu, 2015). Generalmente, estos enfocan su visión desde la perspectiva de las limitaciones y las posibles implicaciones (generalmente sociales) del análisis de datos masivos. Según ellos, *big data* ha abierto una nueva brecha en el acceso al conocimiento, que divide territorios en función de su riqueza de infraestructuras. Dudan de la ética del uso de datos públicos e incluso de la verdadera publicidad de ciertos datos, y consideran que no se garantizan la privacidad y la confidencialidad de los individuos, cada vez más sometidos al control de dispositivos que se extienden en todas las facetas de sus vidas, en la llamada *Internet de las cosas*. Además, consideran que provocará nuevas desigualdades fruto del uso de equipos informáticos capaces de procesar datos a una escala hasta ahora sin precedentes (Lazer *et al*., 2009). Aclaran que este problema ético vinculado al uso de datos personales se manifiesta y se agrava especialmente en el ámbito de los datos personales. Debido a una falta de información y de mecanismos de defensa los ciudadanos pueden perder el control sobre sus datos, encontrarse incapacitados para conocer cómo y quién puede acceder a ellos y de qué modo puede utilizarlos, o simplemente para actuar en pro de la defensa de su privacidad (Baruh y Popescu, 2015; Fairfield y Sthein, 2014; Kalyvas y Oberly, 2014: 33). En esta línea, Mayer-Schönberger y Cukier (2013: 16) señalan una falta de experiencia en la comprensión y la supervisión de los mecanismos de análisis *big data* que puede conllevar perjuicios para los ciudadanos.

Un intento por reducir la ambigüedad que rodea al término se presenta con el trabajo de Ward y Barker (2013). Estos autores presentan un diagnóstico de la problemática en torno al término *big data*, que antes hemos citado. Su estudio analiza un corpus de términos o tendencias vinculados a *big data* del que extraen tres factores comunes (magnitud, complejidad y tecnologías), que posteriormente integran en una nueva propuesta de definición del término. Dichos términos y tendencias se obtienen del estudio de una serie de definiciones de impacto en los últimos años, todas ellas procedentes del sector empresarial. Una de estas definiciones deriva de un análisis de búsquedas realizadas en Google, a través del cual se muestra un listado de términos relacionados con *big data*. Paradójicamente, en este caso Ward y Barker (2013) entienden y emplean la analítica *big data* como una forma de definir el propio término *big data*. Ellos defienden que estos términos o tendencias vinculados se relacionan de forma intrínseca con la propia definición del término *big data*. En este planteamiento reside la asunción previa de que los datos de por sí mismos tienen significado («big data is intrinsically related to data analytics and the discovery of meaning from data» (Ward y Barker, 2013: 2)). Sin embargo, esta es una afirmación que algunos autores consideran resbaladiza (Etlinger, 2014). Apuntan que esta visión hace referencia a una ideología neoliberal que envuelve a

big data, al *deshumanizar* el análisis de datos y desterrar los posibles sesgos relacionados, dotándolo, por tanto, de una falsa apariencia de neutralidad (Baruh y Popescu, 2015). Precisamente, uno de los riesgos que rodean a los datos masivos es el de ligar su análisis a una potencial respuesta ante cualquier cuestión (Galdón, 2014). Etlinger (2014) apunta que, en sí mismos, los datos no tienen significado y que, por el contrario, es su interpretación la que permite darles un significado u otro. Añade que en esta interpretación reside un componente humano y por tanto subjetivo, y recalca que, ante ello, es imprescindible recordar la importancia de las humanidades y de las metodologías cualitativas, que proporcionan el contexto necesario para comprender los datos y permiten conformar un mejor pensamiento crítico. Teniendo en cuenta estas argumentaciones, no parece descabellado señalar una posible asunción errónea de los autores Ward y Barker, al interpretar los términos y tendencias vinculados a *big data* como conceptos intrínsecamente relacionados con él y, por tanto, como una parte integrada en su definición.

Como hemos visto, existen varios motivos por los cuales el desarrollo de una definición única del término *big data* resulta especialmente complejo. Entre ellos destacan su reciente aparición, la multiplicidad de actores y sectores de actividad involucrados que hablan sobre él, o la disparidad de opiniones acerca de su naturaleza y sus posibilidades. A esto se suma la complejidad de definir un concepto, una tarea digna de un profundo estudio de significado.

3. Twitter y *big data*

Actualmente, una gran parte de las informaciones sobre *big data* se difunde a través de las redes sociales y, en particular, a través de la red de *microblogging* Twitter. El objetivo de este trabajo es analizar cómo los mensajes distribuidos a través de Twitter pueden ayudarnos a comprender qué se entiende, de forma general, por *big data*, y contribuir a una definición más acotada del término.

Una de las principales características de las redes sociales son la distribución desigual y altamente jerarquizada de la influencia de los usuarios, que permite su análisis a partir de una pequeña porción de estos, los considerados más influyentes (Guerrero-Solé, Corominas-Murtra y López-González, 2014). Este artículo se apoya en estas características para analizar cómo se distribuye la influencia de los usuarios y sus mensajes en esta conversación, y qué información podemos obtener en cuanto al significado atribuido al concepto *big data*. Pretendemos de este modo dar respuesta a las preguntas de cuáles son los sectores de actividad que más interés tienen en la difusión de información sobre *big data* y en qué sentido van sus mensajes. Además, analizamos cuáles son los temas más frecuentes del discurso dominante a los que se vincula *big data* en Twitter, a través del análisis conjunto de los mensajes y de los términos más empleados entre los tuits analizados.

4. La influencia en Twitter

Twitter, la red de *microblogging* fundada en 2006 que permite la publicación de posts de hasta 140 caracteres, se ha convertido en los últimos años en una de las redes sociales más populares y en uno de los principales objetos de investigación en comunicación. Los estudios sobre Twitter se han centrado en aspectos como la difusión de la información sobre la gripe (Lampos y Critianini, 2010), la predicción de resultados electorales (Tumasjan, Sprenger, Sandner y Welpe, 2010) o del taquillaje de películas antes y después de su estreno (Asur y Huberman, 2010; Deltell, Osteso y Claes, 2013), la polarización política (Guerrero-Solé, 2016) o el análisis de las dinámicas de los índices bursátiles (Bollen, Mao y Zeng, 2011). La influencia de usuarios y mensajes en Twitter ha sido también una de las propiedades más analizadas de la red. Diferentes autores han propuesto algoritmos para la determinación de la influencia tomando en consideración el número de retuits recibidos, las menciones o los seguidores del usuario, entre otras variables (Weng, Lim, Jiang y He, 2010). En este sentido, el número de retuits es el parámetro que se considera más determinante para calcular el impacto de los usuarios en la red. Pero, con independencia del algoritmo utilizado, lo que se observa tanto en Twitter como en el resto de las redes sociales (electrónicas o reales) es la distribución de la influencia siguiendo una ley de potencia (Corominas-Murtra y Solé, 2010) o distribución de Pareto. Eso significa que una pequeña parte de los usuarios poseen la mayor parte de la influencia (y lo mismo pasa con el número de seguidores, el de retuits y menciones recibidos o el de impresiones, los lectores potenciales de un determinado mensaje). Apoyándonos en esta característica, podemos concluir que analizando solo una fracción de los usuarios de una conversación (los más influyentes) y de los mensajes podemos obtener la mayor parte de la información (o, al menos, la más relevante) sobre esta.

5. Objeto de estudio y método

Considerando las grandes inversiones que se están realizando en el campo de *big data*, así como la creciente importancia de este fenómeno en los diferentes sectores sociales y la popularización de Twitter como red de difusión de información en gran parte del mundo, este trabajo se ha propuesto, en primer lugar, analizar cuáles son los usuarios y los mensajes más influyentes en la conversación sobre *big data* en Twitter, para identificar cuáles son los sectores de actividad más interesados en la difusión de información sobre él, y, en segundo lugar, conocer el discurso dominante y los temas de mayor relevancia.

Para ello, se ha recogido una muestra de posts de Twitter que contienen el concepto *big data* o bien la etiqueta #*bigdata*, utilizando la API Search de Twitter.

N_P	Número de posts	162.007
N_T	Número de tuits originales	102.908
N_{RT}	Número de retuits	59.099
U_N	Usuarios únicos	68.195

Tabla 1. Descripción de la muestra de posts sobre #*bigdata* recogidos entre el 23 de noviembre y el 22 de diciembre de 2013

Fuente: *Elaboración propia.*

La elección de la etiqueta y la palabra clave viene justificada por la popularidad y universalidad del término en inglés (sirva de ejemplo la traducción al castellano de la obra de Mayer Schönberger y Cukier (2013), en la que no se traduce el término), y por su brevedad, ya que se compone de solo ocho caracteres, lo que resulta importante debido a la limitación de 140 en la publicación de tuits. La muestra fue recogida entre el 23 de noviembre y el 22 de diciembre de 2013, con un total de 162.007 tuits, a razón de 6.000 tuits diarios. Al tratarse de un trabajo exploratorio, consideramos que una ventana de un mes es suficiente para abordar las cuestiones planteadas. Como se observa en la tabla 1, el número total de usuarios únicos que participaron en la conversación fue de 68.195.

Para cada uno de los mensajes se recogió el identificador único del tuit, el usuario y el nombre completo del autor, el texto del mensaje (que contiene a los usuarios retuiteados, los mencionados, los enlaces externos y las etiquetas), la hora y la fecha de publicación y los datos de geolocalización. Los registros obtenidos fueron importados a una base de datos y procesados para obtener los resultados que se proponía la investigación. Entre los datos calculados estaban el número de veces que un mensaje fue retuiteado y los usuarios que lo retuitearon. A continuación, creamos un registro para cada uno de los usuarios que participaron en la conversación y en el que se recogieron: el número total de tuits y retuits publicados, el número de retuits y menciones totales recibidos, así como los usuarios que lo mencionaron o retuitearon, el número de seguidores y amigos (*followers* y *friends*), el lenguaje de configuración del cliente de Twitter y la descripción y la localización del usuario.

6. Los usuarios y los mensajes más influyentes en la conversación sobre *big data*

A partir de estos datos, aplicamos un algoritmo que tenía en consideración la actividad, los retuits y menciones recibidos y el número de seguidores (Guerrero-Solé y Fernández-Cavia, 2014) para realizar un *ranking* de los usuarios más influyentes en la discusión. En la tabla 2 se muestran los quince usuarios más influyentes según

Usuario	Tipología	Localización	*Rank*	ACT	RT	M	F
Forbes	Medios de comunicación de negocio	NYC	54,609	4	292	864	2.437.300
HarvardBiz	Medios de comunicación de negocio	Boston	23,792	15	1.278	684	1.310.227
TechCrunch	Medios de comunicación de tecnología	Silicon Valley	9,984	1	75	122	3.138.530
Guardian	Medios de comunicación general	Londres	4,499	1	32	102	1.688.149
Intel	Tecnología	California	2,859	2	63	44	2.375.215
WIRED	Medios de comunicación de tecnología	NYC	1,995	2	141	29	2.442.460
SAI	Medios de comunicación de negocio	NYC	1,483	2	28	42	1.287.104
FastCompany	Medios de comunicación de negocio	NYC	1,48	4	46	59	920.319
ForbesTech	Medios de comunicación de tecnología	NYC	1,432	14	274	36	1.027.956
VentureBeat	Medios de comunicación de negocio y tecnología	Silicon Valley	1,411	6	71	244	217.026
FT	Medios de comunicación de negocio	Londres	1,283	3	46	46	995.083
Detikcom	Medios de comunicación general	Indonesia	0,926	2	19	3	6.337.315
Gigaom	Medios de comunicación de tecnología	California	0,76	8	89	141	194.354
EntMagazine	Medios de comunicación de negocio	California, NYC	0,754	1	38	57	501.166
asocialmedia2day	Noticias de medios de comunicación sociales	NYC	0,724	47	349	47	255.818

Tabla 2. Lista de los quince usuarios más influyentes en la conversación sobre *big data* en Twitter, en la que constan su tipología, localización, *ranking*, posts (ACT), retuits recibidos (RT), menciones recibidas (M) y seguidores (F)

Fuente: *Elaboración propia.*

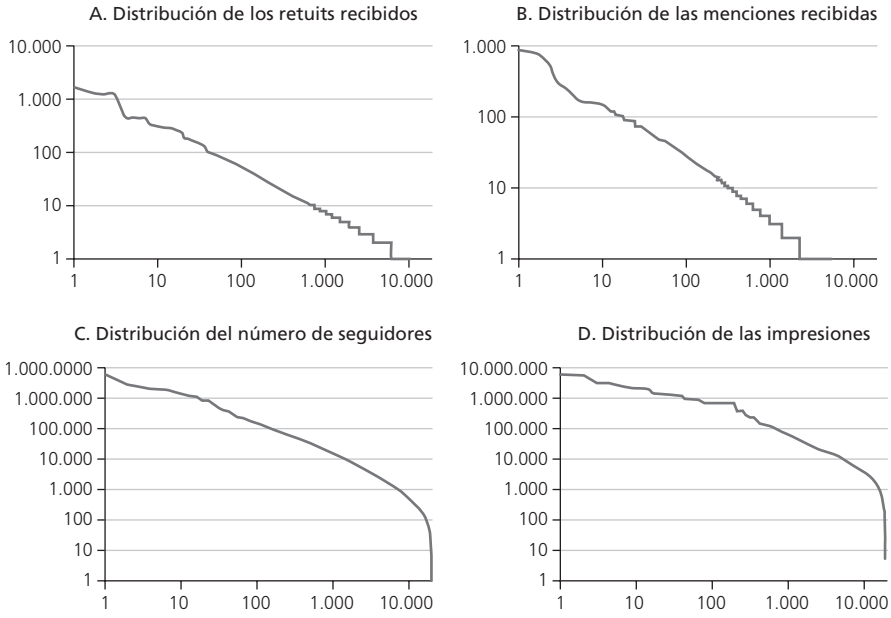

Figura 1. Distribución en escala logarítmica de los retuits recibidos, menciones recibidas, número de seguidores e impresiones de los mensajes

esta jerarquización. Tal y como hemos apuntado antes, la influencia (*Rank*), el número de retuits y menciones recibidos y el número de *followers* siguen una distribución del tipo ley de potencia (figura 1). Para cada uno de los cuatro casos, los exponentes de la ley de potencia son: impresiones (–1,46), RT (–0,91), menciones recibidas (–0,88) y *followers* (–1,76). La aproximación a la ley de potencia es mejor cuanto mayor sea el exponente en valor absoluto, siendo los valores entre 2 y 3 los óptimos.

A su vez, también comprobamos cuáles fueron los mensajes más influyentes (tabla 3), teniendo en cuenta en este caso un único factor, el número de veces que el mensaje fue retuiteado, y descartando aquellos mensajes de usuarios con relativamente pocos seguidores, pero que fueron retuiteados automáticamente y de forma simultánea por su red de seguidores. Consideramos este tipo de mensajes como correo basura.

Además de clasificar los usuarios y los mensajes, calculamos la distribución de los idiomas del cliente de Twitter utilizado (figura 2), así como el número de tuits con enlaces externos y los posts geolocalizados. En el primer caso, comprobamos que de los 102.908 tuits, 91.731 contenían enlace (89 % del total). La utilización de etiquetas y enlaces es una estrategia que se ha observado útil para obtener una mayor redifusión de los mensajes de Twitter (Suh, Hong, Pirolli y Chi, 2010). En el segundo, que solo 1.225 mensajes habían sido publicados por usuarios geolocali-

Usuario	Fecha	RT	Mensaje
HarvardBiz	27/11/2013	140	«Don't invest in big data -- use the data you already have» *http://t.co/yDNCt4eUjK*
Forbes	07/12/2013	139	«Shazam uses big data to predict which music artists will break big in 2014» *http://t.co/8f6dKPqfM8*
HarvardBiz	08/12/2013	128	«How big data will help small businesses» *http://t.co/JI7EHML10p*
HarvardBiz	09/12/2013	94	«Algorithms have their own biases. So what happens when we let them make hiring decision»
HarvardBiz	09/12/2013	89	«Big Data's Biggest Challenge? Convincing People NOT to Trust Their Judgment» *http://t.co/dSZR2Z9RBn*
FastCoExist (Fast Company)	06/12/2013	87	«In The Hospital Of The Future, Big Data Is One Of Your Doctors» *http://t.co/SkyV63MGfp*
HarvardBiz	30/11/2013	82	«To get the most out of your analytics, focus on your top customers» *http://t.co/cyGOOx2*
WIRED	18/12/2013	81	«Big data offers a new tool to help fight human trafficking» *http://t.co/ds4eR5RJKj*
Forbes	04/12/2013	59	«5 reasons why Big Data will crush Big Research» *http://t.co/6llQJBTADz*
HarvardBiz	25/11/2013	54	«How is Big Data Transforming Your 80/20 Analytics?» *http://t.co/NmBjKMMxfj*

Tabla 3. Lista de los diez mensajes más retuiteados en la conversación sobre *big data*

Fuente: *Elaboración propia.*

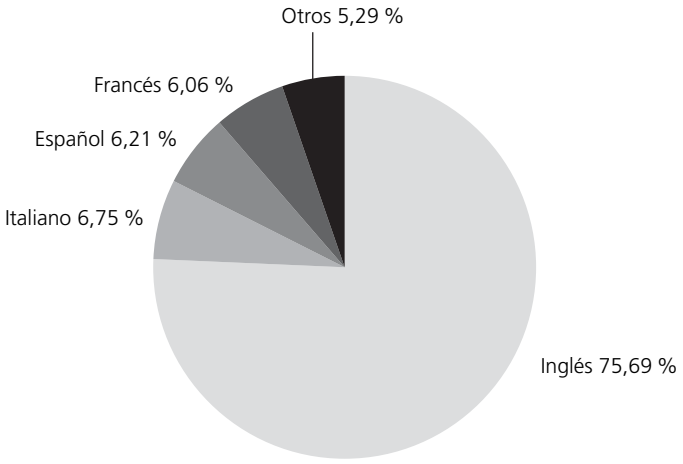

Figura 2. Porcentaje de mensajes por idioma del cliente de Twitter

zados, por lo que obviamos analizar su procedencia ya que los consideramos poco significativos.

7. Análisis del tema dominante en la conversación sobre *big data*

La última fase del análisis consistió en la identificación de las palabras más repetidas en la conversación, considerando únicamente los tuits y dejando aparte los retuits. En este caso no consideramos la ponderación de las palabras en función del *ranking* de los usuarios. El propósito de este análisis iba más allá del simple recuento y pretendía completar el análisis de los mensajes más influyentes para identificar el discurso dominante sobre *big data* en Twitter, a partir del análisis de los términos que eran más utilizados por los usuarios. En la tabla 4 podemos ver cuáles fueron los veinte términos más utilizados.

Término	Frecuencia
Analytics/Analysis	13.782
You/Your	9.624
How	7.695
Marketing/Market	5.935
Cloud	5.724
Business	4.567
Will	4.466
Use	4.357
Can	4.135
Predict	3.373
What	3.363
Hadoop	3.134
IBM	2.439
Help	2.306
Why	1.051
Company	1.955
Future	1.862
Next	1.759
Social	1.660
World	1.645

Tabla 4. Lista de los veinte términos más utilizados en la conversación sobre *big data*
Fuente: *Elaboración propia.*

8. Conclusiones de la investigación

8.1. Los usuarios más influyentes

El método de análisis de los tuits aplicado en este estudio nos ha permitido detectar cuáles son los usuarios más influyentes en la conversación analizada en este estudio sobre #*bigdata* en Twitter. Los resultados muestran que la mayoría de estos usuarios corresponden a empresas norteamericanas (con excepción de dos británicas y una indonesia) ubicadas en Nueva York y California, y excepto el fabricante de tecnología Intel, prácticamente todos son medios de comunicación sobre tecnología y negocios. Precisamente los medios de comunicación, junto con las celebridades, son considerados desde los inicios de Twitter como los usuarios con mayor influencia (Kwak, Lee, Park y Moon, 2010). Así, pues, podemos constatar que los medios financieros son uno de los sectores más influyentes en la conversación sobre *big data*. El hecho de que sea este sector y no otro el que domine la conversación repercute en el tipo de información más influyente, centrada en las estrategias de análisis de datos para obtener rendimientos económicos, ventajas competitivas y toma de decisiones.

Otra de las características de la red de usuarios es que las informaciones de los más influyentes son, por definición, las más redifundidas por el resto de la red. En cambio, estos no redifunden prácticamente ningún otro contenido que no sea el propio. Es decir, los más influyentes no establecen una relación de reciprocidad con ninguno de los usuarios que retuitean su información, por lo que no contribuyen a que estos sean también influyentes. Se reproduce, de este modo, el esquema tradicional de medios unidireccionales, en el que solo los mensajes de unos pocos son redifundidos. Si los usuarios más influyentes retuitean algún mensaje, normalmente es de usuarios que forman parte de su misma organización (es el caso de Forbes, que retuitea a ForbesTech, o de FastCompany, que lo hace de FastCoExist). Podemos ver en la figura 3*b*, en la que se muestra la red formada por los usuarios que se retuitean entre sí, que esta es muy fragmentada y presenta clústers con muy pocos usuarios. No aparecen en ella ninguno de los cincuenta usuarios más influyentes. En cambio, la figura 3*a* nos muestra la red de los usuarios que retuitean a los más influyentes. Podemos observar cómo estos son retuiteados por un gran número de usuarios de la red.

8.2. Los mensajes más influyentes

En cuanto a los mensajes analizados, hemos comprobado, por un lado, que aquellos identificados como más influyentes provienen también de algunos de los usuarios más influyentes, como son HarvardBiz, Forbes, Fast Company y Wired. Además, hemos podido comprobar que la mayoría de los mensajes más influyentes se centran en los mismos aspectos y dibujan un escenario similar al identificado mediante el listado de los veinte términos más recurrentes. Esto nos ha permitido hacer una reconstrucción de cuál es el tema dominante en la conversación analizada: el uso del análisis de grandes datos como una nueva herramienta capaz de ayudar

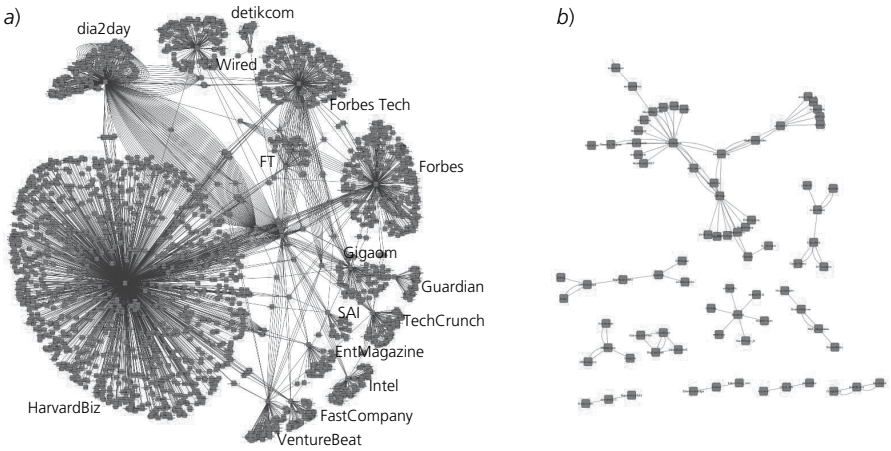

Figura 3. Red de retuiteadores de los quince usuarios más influyentes (*a*) y red de usuarios que se retuitean mutuamente (*b*) en la conversación sobre *big data*

a las empresas a tomar decisiones, predecir el futuro y, por lo tanto, poder mejorar su producción, su logística o sus estrategias de comunicación y venta de productos y servicios. Esta lista de términos también nos ha servido para identificar, de forma independiente al análisis de usuarios, a dos de los principales actores tecnológicos en el campo de #*bigdata*, cuyos nombres se han repetido con una frecuencia de 3.134 y 2.439 veces respectivamente: por un lado, Hadoop, la principal plataforma de análisis de grandes cantidades de datos, y por el otro, el fabricante de equipos y servicios informáticos IBM, el líder indiscutible en este campo.

En el sentido contrario, la presencia de mensajes y de términos relacionados con posturas críticas frente a #*bigdata* es menor. Dos de los conceptos más utilizados desde la perspectiva crítica son los de *privacidad* y *vigilancia*, que aparecen con una frecuencia de 950 y 163 veces respectivamente en el corpus de mensajes analizados. A pesar de ello, hay que destacar que los mensajes de uno de los usuarios más influyentes (HarvardBiz), autor de la mitad de los mensajes más retuiteados, tiene un discurso que no está completamente alineado con el dominante, y está también dirigido a animar a las empresas a fijarse en activos que ya poseen (como sus propios datos), o a poner en evidencia los sesgos de los algoritmos y sus implicaciones en la toma de decisiones tan sensibles como la contratación de personal.

9. Discusión

El método aplicado nos ha permitido elaborar una lista de los usuarios y otra de los mensajes más influyentes e identificar los términos más empleados en esta conversación. Esto nos ha servido a su vez para identificar al sector de los medios finan-

cieros y las empresas tecnológicas como los principales sectores interesados en la difusión de información sobre *big data* y para determinar una clara repercusión de este hecho en el tipo de información más influyente, vinculada a la implementación de mejoras estratégicas y logísticas y, por lo tanto, a la obtención de beneficio en el ámbito empresarial.

Por un lado, estos resultados hacen patente que existe una fuerte disparidad de los discursos y las visiones acerca del fenómeno *big data*. Por otro, demuestran la existencia de un fuerte discurso mayoritario, que se vincula con la visión más utilitarista de las que contextualizábamos al inicio: hemos encontrado que los usuarios más influyentes vinculan al desarrollo de *big data* una modificación de las lógicas empresariales, enfatizan la usabilidad de los datos como una nueva forma de obtención de valor y acentúan la predicción y la toma de decisiones basadas en datos como dos nuevas grandes oportunidades para el sector empresarial, la seguridad y el progreso. De forma contraria, como hemos dicho, el usuario más destacado de la lista de más influyentes (HarvardBiz) apela a una visión más escéptica que los demás, especialmente sobre las posibilidades que se proyectan. En su discurso acentúa algunos de los desafíos ligados a *big data*, se muestra contrario a la inversión en él y propone recursos alternativos de mayor efectividad. Sin embargo, entre los mensajes y usuarios más influyentes no se refleja la visión crítica, que, como decíamos en la introducción, es otra de las visiones más defendidas acerca de este fenómeno y resulta contraria a la del discurso mayoritario. En cualquier caso, sí se han encontrado términos repetidos con una frecuencia suficiente, que acreditan la existencia de esta otra visión.

De entre lo expuesto en este trabajo cabe resaltar, por una parte, que *big data* tiene una gran potencialidad para mejorar ciertos aspectos de la sociedad. La predicción y la elaboración de diagnósticos precisos puede aportar grandes avances, pero parece necesario contemplar el uso de datos desde una perspectiva responsable con la privacidad de las personas, y tener en cuenta las limitaciones propias de los datos y también del posterior procesamiento e interpretación de los mismos. Otra cuestión relevante atañe a las posibilidades de la analítica predictiva. Mayer Schönberger y Cukier (2013) señalan que, si bien la cantidad de información recogida sobre las personas es cada vez mayor, la idea de predecir sus conductas o comportamientos en base a ella guarda relación con concepciones de la naturaleza humana vinculadas a paradigmas como el conductista, el determinista o el mecanicista, según los cuales el ciudadano es visto de forma despersonalizada y facultades como el libre albedrío se ven perturbadas.

10. Limitaciones

Una de las principales limitaciones de este trabajo es que la muestra de mensajes sobre #*bigdata* no es completa, ya que se recogieron un número de alrededor de

6.000 tuits por día. Esta muestra está, además, sujeta a los posibles sesgos de la API Search de Twitter, empleada para la recolección de datos. En este sentido, y a pesar de que podemos considerar que 160.000 mensajes es una muestra suficiente para obtener conclusiones válidas respecto al debate sobre #*bigdata*, estamos trabajando en la obtención de una muestra mucho mayor y más completa, que nos permita obtener conclusiones más definitivas, así como observar cuál es la evolución del discurso y la dinámica de la influencia de los usuarios a lo largo del tiempo. Otro de los aspectos que deben mejorarse de cara al interés de este estudio, y en coherencia con la crítica realizada en el estudio de Ward y Barker (2013), es el del análisis del discurso de los mensajes con herramientas que nos permitan afirmar con mayor precisión cuál es el sentido de cada uno de ellos. Finalmente, también debemos tener en cuenta la desigual distribución de la penetración de Twitter en el mundo. Una de las posibles consecuencias de este hecho es que puede eclipsar las contribuciones de los usuarios y mensajes procedentes de países como la India, China o Rusia, que pueden estar desarrollando estrategias de análisis de grandes cantidades de datos, y cuyas informaciones fluyen en otro tipo de plataformas como Facebook o la red social china Sina Weibo. Además, se ha de contemplar también el problema del desigual acceso al conocimiento e infraestructuras, conocido como *brecha digital*, que mencionábamos al inicio de este trabajo y que favorece hechos como el demostrado en este artículo, relativo a los lugares de procedencia tanto de las informaciones como de los usuarios más influyentes (América del Norte).

Así, a pesar de estas limitaciones, lo que sí que podemos afirmar es que, gracias a sus potencialidades, *big data* es y será una apuesta de futuro, no solo para las empresas, sino también para las instituciones públicas y los gobiernos. Sirva de ejemplo la reciente creación del Alan Turing Institute en el Reino Unido. El gobierno británico invertirá 42 millones de libras en cinco años en un proyecto sobre *big data* que, en palabras de George Osborne, su rector, va a permitir a las empresas mejorar sus procesos de producción, orientar mejor sus estrategias de venta y proveer servicios más eficientes (BBC News, 2014), en clara sintonía con el mensaje que hemos extraído del análisis en Twitter.

Notas

[1] Dirección de correspondencia: Sara Suárez. Roc Boronat, 138. E-08018, Barcelona, UE.

Bibliografía

Asur, S.; Huberman, B. A. (2010). «Predicting the future with social media». *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, p. 492-499. DOI: 10.1109/WI-IAT.2010.63.

Baruh, L.; Popescu, M. (2015). «Big data analytics and the limits of privacy self-management». *New Media & Society*, p. 1-18. DOI: 10.1177/1461444815614001.

BBC News (2014). «Alan Turing Institute to be set up to research big data». <http://www.bbc.com/news/technology-26651179>.

Bollen, J.; Mao, H.; Zeng, X. (2011). «Twitter mood predicts the stock market». *Journal of Computational Science*, 2, p. 1-8. DOI: 10.1016/j.jocs.2010.12.007.

Boyd, D.; Crawford, K. (2012). «Critical questions for big data». *Information, Communication & Society*, 15, p. 662-679. DOI: 10.1080/1369118X.2012.678878.

Cox, M.; Ellsworth, D. (1997). *Application controlled demand paging for out of core visualization*. Report NAS-97-010, julio 1997. Moffet Field: NASA Ames Research Center.

Davenport, T. H. (2014). *Big data at work: Dispelling the myths, uncovering the opportunities*. EUA: Harvard Business Review Press.

Deltell, L.; Osteso, J.-M.; Claes, F. (2013). «Twitter en las campañas comunicativas de películas cinematográficas». *El Profesional de la Información*, 22, p. 128-134. DOI: 10.3145/epi.2013.mar.05.

Durán Segura, M.; Mejías Peligro, J. F. (2014). «Conocimientos y comportamientos de los usuarios de la red social Facebook relacionados con la privacidad». *Ámbitos: Revista Internacional de Comunicación*, 26: Infoxicación. ISSN digital: 1988-5733.

Etlinger, S. *Susan Etlinger: What do we do with all this big data?* [Videoconferencia TED] (septiembre 2014). Recuperado el 20 de marzo de 2015 de: <http://www.ted.com/talks/susan_etlinger_what_do_we_do_with_all_this_big_data?#t-575588>.

Fairfield, J.; Shtein, H. (2014). «Big data, big problems: Emerging issues in the ethics of data science and journalism». *Journal of Mass Media Ethics: Exploring Questions of Media Morality*, 29:1, p. 38-51. DOI: 10.1080/08900523.2014.863126.

Galdón, G. *Entrevista a Gemma Galdón, experta en privacidad en la red*. Vídeo de Youtube (10 diciembre 2014). Recuperado el 20 de marzo de 2015 de: <https://www.youtube.com/watch?v=YHfopl714hg>.

Guerrero-Solé, F. (2016). «Community detection in political discussions on Twitter. An application of the Retweet Overlap Network method to the Catalan process towards independence». *Social Science Computer Review*. DOI: 10.1177/0894439315617254.

Guerrero-Solé, F.; Corominas-Murtra, B.; Lopez-Gonzalez, H. (2014). «Pacts with Twitter. Predicting voters indecision and preferences for coalitions in multiparty systems». *Information, Communication & Society*, 17 (10), p. 1280-1297. DOI: 10.1080/1369118X.2014.920040.

Guerrero-Solé, F.; Fernández-Cavia, J. (2014). «Activity and influence of destination brands on Twitter: A comparative study of nine spanish destinations». *Information and Communication Technologies in Tourism 2014*. Springer International Publishing, p. 227-236.

Hoy, M. G.; Milne, G. (2013). «Gender differences in privacy-related measures for young adult Facebook users». *Journal of Interactive Advertising*, 10 (2), p. 28-45. DOI: 10.1080/15252019.2010.10722168.

Kalyvas, J. R.; Overly, M. R. (2014). *Big Data: A business and legal guide*. Nueva York: Taylor & Francis Group, LLC.

Kwak, H.; Lee, C.; Park, H.; Moon, S. (2010). «What is Twitter, a social network or a news media?». *The International World Wide Web Conference Committee (IW3C2)*, p. 1-10. DOI: 10.1145/1772690.1772751.

LAMPOS, V.; CRISTIANINI, N. (2010). «Tracking the flu pandemic by monitoring the social web». *2010 2nd International Workshop on Cognitive Information Processing, CIP2010*, p. 411-416. DOI: 10.1109/CIP.2010.5604088.

LANEY, D. (6 febrero 2001). «File 949. 3D Data Management: Controlling Data, Volume, Velocity and Variety». *Application Delivery Strategies* [Stamford: META Group Inc] (6 febrero). <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf> [Consulta: 15 diciembre 2014].

LAZER, D.; PENTLAND, A.; ADAMIC, L.; ARAL, S.; BARABÁSI, A.; BREWER, D.; CHRISTAKIS, N.; CONTRACTOR, N.; FOWLER, J.; GUTMANN, M.; JEBARA, T.; KING, G.; MACY, M.; ROY, D.; VAN ALSTYNE, M. (2009). «Computational social science». *Science*, 323, p. 721-723. DOI: 10.1126/science.1167742.

MANOVICH, L. «Trending: the promises and the challenges of big social data». En: GOLD, M. G. (2012). *Debates in the digital humanities*. Arizona: University of Minessota Press, p. 460-475.

MAYER-SCHÖNBERGER, V.; CUKIER, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Boston; Nueva York: Houghton Mifflin Harcourt.

MINELLI, M.; CHAMBERS, M.; DHIRAJ, A. (2013). *Big data, big analytics: Emerging business intelligence and analytic trends for today's businesses*. Hoboken, NJ: John Wiley & Sons, Inc. DOI: 10.1002/9781118562260.

SHROEK, M.; SHOCKLEY, R.; SMART, D. J.; ROMERO-MORALES, D.; TUFANO. P. (2012). *Analytics: el uso de big data en el mundo real. Cómo las empresas más innovadoras extraen valor de datos inciertos*. Informe ejecutivo. IBM Global Business Services Business Analytics and Optimisation. <http://ibm.co/1APKffj> [Consulta: 6 mayo 2015].

SUH, B.; HONG, L.; PIROLLI, P.; CHI, E. H. (2010). «Want to be retweeted? Large scale analytics on factors impacting retweet in Twitter network». *Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust*, p. 177-184. DOI: 10.1109/SocialCom.2010.33.

TUMASJAN, A.; SPRENGER, T.; SANDNER, P.; WELPE, I. (2010). «Predicting elections with Twitter: What 140 characters reveal about political sentiment». ICWSM, p. 178-185. DOI: 10.1074/jbc.M501708200.

WARD, J. S.; BARKER, A. (2013). «Undefined by data: A survey of big data definitions». *arXiv.org*, 2. <http://arxiv.org/abs/1309.5821>.

WENG, J.; LIM, E.; JIANG, J. (2010). «TwitterRank: Finding topic-sensitive influential twitterers». *New York, Paper 504*, p. 261-270. DOI: 10.1145/1718487.1718520.

2

Suárez-Gonzalo, Sara; Mas-Manchón, Lluís; Guerrero-Solé, Frederic (2019). Tay is you. The attribution of responsibility in the algorithmic culture, *Observatorio (OBS*), 13*(2): 1-14. doi: https://doi.org/10.15847/obsOBS13220191432.

ISSN electrónico: 1646-5954.

Observatorio (OBS*) Journal, (2019), 001-014 1646-5954/ERC123483/2019 001

Tay is you. The attribution of responsibility in the algorithmic culture.

Sara Suárez-Gonzalo*, Lluís Mas-Manchón*, Frederic Guerrero-Solé*

*Universitat Pompeu Fabra, Spain

Abstract

Social media have changed the communication practices by creating an acute need for continuous interaction. The use of social chatbots is growing as an effective way to communicate with publics. Bots have become social actors and then, someone must account for their actions. Since responsibility is bounded to agency and rationality, it cannot be directly attributed to bots. Who should be held responsible for non-human beings' actions, particularly when the consequences of these actions are negative?

We address this controversy from both theoretical and empirical perspectives. Firstly, we discuss the adequacy of the notions of moral responsibility and accountability regarding non-human artificial agents, as they are ruled by complex, intentionally opaque and unpredictable interactions and processes. We do it from the two approaches currently predominant: context-dependent and structuralist. Secondly, we draw on the assumption that the failure of a computer system is an opportunity to gain knowledge about the interested powers behind its design and functioning. Then, taking the concept of media frame as an implicit way of spotting the agent of the story, we perform an exploratory analysis on how responsibility was attributed by the media in the paradigmatic case of the transformation of Tay, a chatbot launched by Microsoft in 2016, turned into a racist, Nazi and homophobic hate speaker.

Our results illustrate the difficulties media experienced in consistently attributing the responsibility for the chatbots' malfunction. Results show the discourse is, in general, simplistic, non-critical and misleading, and tends to depict a reality that favors business's interests. We conclude that, while all the actors interacting with the chatbot share the responsibility of its actions, it is only Microsoft who must account for these actions, both retrospectively and prospectively.

Keywords: Chatbots, big social data, artificial intelligence, Twitter, algorithmic culture, accountability, attribution of responsibility, Tay, hate speech.

Submitted: 22nd November 2018

Accepted: 31st March 2019

How to quote this article:

Suárez-Gonzalo, S., Mas-Manchón, L, Guerrero-Solé, F. (2019). Tay is you. The attribution of responsibility in the algorithmic culture. *Observatorio*, 13(2), 1-14.

Introduction

Social media have challenged the traditional one-to-many communication paradigm (Castells, 2009; van Dijk, 2013) and have lead institutions and organizations to adapt to a new environment in which personalized interactions with thousands, even millions of people, are required (Neff & Nagy, 2016). Since human actors cannot perform such a large amount of interactions, companies have developed the so-called chatbots, technologies based on big data analytics and machine learning that conversationally interact with users, mainly on social networks (Ferrara, Varol, Davis, Menczer & Flammini, 2016). Social

network sites (SNS) are particularly suitable platforms for the collection of great amounts of social data (Tufekci, 2014; boyd & Ellison, 2007) that can be processed in real-time by machine learning technologies and become a source for machine-generated content (Nichols, 2010). This content is the basis for personalized interactions carried out by chatbots that emerge as relevant non-human social actors in SNS.

Scholars have begun to scrutinize the potential negative impact of bots on society. From a critical perspective, these technological artifacts are characterized by the opacity and black-boxed nature of the algorithms that rule their actions (Pasquale, 2015). Due to the enormous complexity of such algorithms, scholars have put the focus on cases of unsatisfactory functioning as a way to gain knowledge about their inner characteristics and effects (Karppi & Crawford, 2016). This knowledge is essential when dealing with highly problematic concepts such as agency, accountability or the attribution of responsibility in the context of the algorithmic culture (Hallinan & Striphas, 2015).

The aim of this work is to contribute to the debate about chatbots' acts responsibility and accountability from both theoretical and empirical perspectives. On the one hand, we examine the adequacy of traditional notions of responsibility and accountability in the context of the algorithmic culture. On the other, this research explores the discourse of media outlets in such a case in which computational systems fail. We perform an exploratory frame analysis (Entman, 1993; Semetko & Valkenburg, 2000) of the news stories on Tay's failure, a Twitter chatbot launched by Microsoft Corporation in 2016. Since after a 24 hours period of interaction with Twitter users the bot's messages turned into racist, homophobic and sexist hate speech, we pay a special attention to how media attributed responsibility of this misbehavior. Finally, we discuss whether the algorithmic culture is influencing the construction of media discourse about chatbots' agency and responsibility.

From user to machine generated content

The rapid development of information technologies at the end of the 20th century made the volume, variety and velocity of data grow dramatically (Laney, 2001). In 1997 Michael Lesk predicted that in the year 2000 there would be enough space of storage to register almost any expression of human activity. He also warned that such a large amount of data could not be inspected by humans in the future, and a continuous automatic evaluation would be a requisite to decide what portions of information should get "the precious resource of human attention" (Lesk, 1997: 9). Two decades later, Lesk's predictions have been widely confirmed, and nowadays we live in a big data ecosystem (boyd & Crawford, 2011), being the *datafication* of everyday life an increasingly pervasive trend (Baruh & Popescu, 2015; Suárez-Gonzalo, 2017). In this sense, the size and complexity of datasets undermines humans' capacity to deal with data and to make sense of them (Baldi, 2017; Shalev-Shwartz & Ben-David, 2014). According to Hallinan and Striphas (2016: 119), a new algorithmic culture has emerged, which lies in "the use of computational processes to sort, classify, and hierarchize people, places, objects, and ideas, and also the habits of thought, conduct, and expression that arise in relationship to those processes'.

Under the name of artificial intelligence (AI), highly sophisticated computational techniques have been developed to replace humans in relevant activities (Carbonell, Michalski & Mitchell, 1984), such as content creation, information management and distribution and decision-making (Marsland, 2015). Machine learning is the current paradigm in the field of AI (Bostrom, 2015) that trains computers to learn. It allows computers to adapt their actions to the changes in the environment (Shalev-Shwartz & Ben-David, 2014),

and to discover complex structures and patterns in high-dimensional datasets (LeCun, Bengio & Hinton, 2015). For Nath and Levinson (2014), machine learning can be understood as algorithms that constantly improve their outcomes by means of available data.

The nature of social chatbots

Social chatter robots (chatbots) are a particular case of this new generation of machine learning technologies that make use of social media data to generate natural language outputs and engage in conversations with human users (Griol, Sanchis de Miguel & Molina, 2014). They are, nowadays, an effective way to communicate with users (Chakrabarti & Luger, 2015). Due to the enormous amount of data spread by users, SNS have become particularly thriving ecosystems for the development of chatbots. In the past few years, chatbots have settled in social networks (Sandvig, Hamilton, Karahalios & Langbort, 2016; Ferrara et al., 2016) and are holding strategic roles in organizations' communication actions (Neff & Nagy, 2016). In this sense, communication technology corporations such as Apple, Samsung, Microsoft or Facebook have already developed their own chatbots. They have also played a relevant role in political events, such as the latest United States presidential election campaign (Kollani, Howard & Wooley, 2016).
However, chatbots can also contribute to amplify old biases in society and are acquiring perilous roles in public life (Caplan & boyd, 2016). Research has shown that can they lead to algorithmic discrimination (boyd, Levy & Marwik, 2014) and are capable of swaying public opinion (Marechal, 2016), perpetuating social damaging stereotypes (Sandvig *et.* al, 2016), destabilizing financial markets (Karppi & Crawford, 2016), or amplify the spreading of misinformation (Ferrara et al, 2016) and hate speech (Marwick & Lewis, 2017), among others. Additionally, corporations and governments foster the opacity of such algorithms through real secrecy, legal secrecy and intentioned obfuscation (Pasquale, 2015: 2).
Thereby, considering the complex and opaque nature of algorithms in chatbots, and the fact that machine-learning technology takes advantage of the contents published by users, a question emerges: who is responsible of chatbots' behavior when they fail?

The responsibility gap: attributing responsibility to artificial beings in a networked society

Responsibility has been traditionally bounded to actions with concrete intentions (Asaro, 2012; Hellström, 2013) and significant consequences (Fisher, 1999). Responsibility has been usually attributed to individuals, groups of individuals or institutions (referred as the "agent") when their actions have an effect on others (referred as the "patient") (Floridi & Sanders, 2004). The attribution of responsibility requires the agent to be rational, as well as to have intention and agency (Mitcham, 2014; Guilbeault, 2016). Consequently, responsibility establishes a link between agents and patients and organizes social relations.
Accountability is the assumption of responsibility by the agent. Bovens defines it as "a social relationship in which an actor feels an obligation to explain and to justify his or her conducts to some significant other" (2005: 184), especially when it comes to actions with negative consequences. Generally, accountability is part of the relationship between society and the state (Caplan & boyd, 2016). According to Rosenblat, Kneese and boyd (2014), it is fundamentally about checks and balances to power. It has a retrospective dimension (being blamed or punished for an action), which is the most commonly accepted, and a

prospective one (defining obligations and duties related to that action). Both responsibility and accountability are dependent on identifying the agent of the action and whether her or his actual intention is rationally aligned with the consequences of this action (Groom et al., 2010).

In digital environments such as SNS, in which chatbots become algorithmically controlled actors that learn from others' behaviors, agency and intention are not easily attributed. Questions such as whether a chatbot can be considered as a rational agent or not, or its actions as intended, become problematic. Besides, in modern sociotechnical relations, tasks are distributed between human and non-human entities in a way that unpredictably affects each other. This makes it hard to identify the agent of a certain action.

As noted by Kroll et al. (2017), social bots are peculiar black boxes in which the inner workings are either too complicated or based on randomness, and so the outcomes become difficult to foresee. Following Matthias (2004), while the operators of learning machines are not capable to predict the future behavior of such machines, they cannot be held responsible for their actions. Therefore, intentionality, causality and the agent-patient link become hard to define. As the complexity and autonomy of learning machines keep growing, humans cannot continue to be directly responsible for them. In some way, humans lose control over them, and bestow the decision-making process to the machines themselves. In such cases, society must address what Matthias calls a "responsibility gap". Gotterbarn (2001) and Waelbers (2009) add two pervasive misconceptions about technology and responsibility that complicate the attribution of responsibility in such cases: the alleged ethical neutrality of technological artifacts; and the predominant reductionist understanding of responsibility, which only considers its retrospective conception.

All this complexity has lead several authors to notice that the case of artificial beings requires rethinking the very concepts of responsibility and accountability so to make them applicable to networked environments (boyd, Levy & Marwick, 2014). Several authors have also emphasized the need for algorithmic transparency (Kemper & Kolkman, 2018), external control of algorithmic processes (Pasquale, 2015; boyd, 2016) and to design them according to previously agreed values (boyd, 2016) such as the five defined by Diakopoulos and Friedler (2016): responsibility, explainability, accuracy, auditability and fairness.

There are interesting contributions regarding the intentionality and agency of artificial beings, which can be classified into two main approaches regarding the attribution of responsibility and the accountability of chatbots's actions. One is the context-dependent approach: responsibility corresponds to the environment with which the bot interacts, and so its assumption disperses among all actors. The other is the structuralist approach: assuming the responsibility of bot's actions corresponds to the forces involved in the design and management of the bot.

Regarding the context-dependent approach, Floridi (2014) poses that when an artifact learns from the context in which it performs, intentionality spreads through the different relationships and outer interests involved in the interaction. In this same line, Introna (2014) draws on Foucault to develop an interactional concept of intentionality, defined as the inseparable interaction between technical artefacts ("dispositifs") and humans. According to van Dijk (2013), given that the environment as a whole can be considered as the input of social bots and also that it is based on simple interactions that define each other's identity, agency could be considered also a networked concept. Similarly, Neff and Nagy (2016: 4916) develop the concept of symbiotic agency, defined as: "what users, actors, and tools do when interacting with complex technological systems […] In other words, what people say about bots influences, what people can do with them and what capacities the bots have for social action".

Regarding the structuralist approach, Johnson (2006) argues that although computer technologies are not intentional, they do have intentionality, always related to that of their designers and users. She emphasizes the need to consider the social, political and institutional forces interested in shaping technological developments. In this same line, Ford, Dubois and Puschmann (2016) pose that chatbots' actions should be accounted by a set of different interests participating in the co-creation of these chatbots. Through a quantitative and qualitative study on Youtube, Rieder, Matamoros-Fernández and Coromina (2018) highlight the intricate mesh of mutually constitutive agencies that play a role in algorithm's functioning. Rieder (2018), moreover, examines the relationship between governmentality and computing and notes the importance of dealing with computers as political tools in the hands of interested actors or think tanks. Murthy *et al.* (2016) note that bots are created by social, political and economic systems of power (an idea also supported by Karppi & Crawford, 2016).

@TayandYou, a paradigmatic case of study

On Saturday, March 23rd 2016, Microsoft launched Tay*,* a new chatbot on Twitter. The bot was designed to simulate a young American millennial girl, with the purpose of informally interacting with Twitter users, millennials preferably, and conduct research on conversational understanding. As stated by Microsoft (2016), Tay was built "by mining relevant public data and by using AI and editorial developed by a staff including improvisational comedians". In order to have the most personalized and satisfactory experience, Microsoft warned users that the more they chatted with Tay, the smarter she would get. However, hundreds of users started tweeting with the chatbot by making misogynistic and racist comments. Because of its machine-learning nature, Tay's messages, tone and vocabulary also became racist and misogynistic dramatically. A few hours later and as a result of Tay`s inappropriate behavior, Microsoft removed the chatbot arguing that it suffered a malicious attack (Lee, March 25th, 2016). Three days later, on March 30th, Microsoft launched a renewed version of Tay. However, its behavior soon became even worse than before, and Microsoft definitively removed the chatbot from Twitter.

Media framing of Tay's event

As pointed out by Druckman and Bolsen (2011), public opinion plays a critical role on how people perceive emergent technologies. In this regard, the way media portrays a new technology is a definitive factor for its success. Spicer (2005) pointed out that the way complex digital technologies will be used is shaped during their process of social inclusion by political and economic forces. Stahl (1995), for his part, conducted a major study on *Time*'s framing of the first IBM personal computers. Results show that magical and religious language was commonly used in news media as a plan for legitimizing computers' black boxed condition. Besides, he argues that machines are frequently portrayed (antrophormized) as the active partners in human-computer relationships, making people feel powerless facing technology. Stahl concludes that, since not all social groups are equally able to define new technologies, media tend to stabilize and close the technological business' frame. That is: they promote business' definitions of technology. As noted by Puschmann and Burgess (2014), media discourse on science and technology usually tends to overgeneralize and subjugate the reality to power disputes. Campbell (2010) maintains

that risk has also been frequent in media representations of emerging technologies, in particular when these technologies challenge the stability of other sociotechnical discourses.

Media outlets immediately reported on the failure of Tay. Assuming that media discourse depicts a particular understanding about artificial intelligence, machine learning, and chatbots, our main aim is to perform an exploratory analysis of how media framed and attributed the responsibility of the transformation of Tay. As defined by Entman (1993), framing involves selection and salience to prescribe and promote interpretations and evaluations of issues in media. Frames draw attention toward certain aspects of reality while marginalizing others (Lawrence, 2000). While the attribution of responsibility is conceptualized as a process of explicitly spotting the primary agent of certain phenomenon (the ultimate cause), framing is well known theory on how the media shed light into some direction regarding any stories' agents, hence responsibility can only be derived from framing implicitly. Thus frames must just be considered as a sort of premise for the attribution of responsibility. We will not go deeper in this insight.

Many scholars in the communication field have proposed diverse taxonomies of media frames. In particular, Semetko and Valkenburg (2000) identified the five prevalent frames in previous researches on news media content and systematized their identification in their classic work on European politics. These frames are: F1. *Conflict*: emphasizes the existence of conflicts between individuals, groups, or institutions as a means of capturing audience interest (it can induce public cynicism and mistrust); F2. *Human interest*: brings a human face or an emotional angle to the presentation of an event, issue, or problem: is supposes an effort to personalize, dramatize or "emotionalize" the news in order to capture and retain audience interest; F3. *Economic consequences*: reports an event, problem, or issue in terms of the consequences it will have economically on an individual, group, institution, region, or country; F4. *Morality*: puts the event, problem, or issue in the context of religious tenets or moral prescriptions, often by means of an indirect reference. It may contain moral messages or offer specific social prescriptions about how to behave; and finally, the one which they identified as the predominant one, F.5. *Attribution of responsibility*: presents an issue or a problem in such a way to attribute responsibility for its cause or solution to either an institution, individual or group. It encourages people to offer individual-level explanations for social problems.

Semetko and Valkenburg elaborate on a deductive, rather than an inductive (Gamson, 1992), approach to framing. This deductive approach involves having a clear idea of the types of frames that are likely to appear in the news and, afterwards, quantify them in the sample of news. Unlike the inductive approach, which is arduous to apply as it involves analyzing the news with an open view, the deductive method is easily replicable. Because of that, it has been employed by a multitude of researchers, especially in relation to media news on political issues and crisis communication (Coman & Cmeciu, 2014; An & Gower; 2009).

In view of previous theoretical considerations and the role played by media outlets in shaping public opinion, we tried to answer the question about how news media framed Tay's failure, and how they attributed the responsibility of this failure. For this purpose, we performed an exploratory research by collecting and analysing a sample of news about the Tay event from April to November 2016, when the number of news stories about the case falls significantly. As for the sample selection, we draw on the ranking published by Comscore MMX Multi Platform of the most read digital newspapers in Spain during the period analyzed. Then, we gathered the news published by the seven generalist newspapers of this list that published two or more news fully dedicated to Tay's event during that period. Moreover, we added to the sample the two international online dailies (The Guardian, The New York Times) and the three

technology newspapers (The Verge, Wired, ZD Net) of reference in Spain that published the greatest number of news about Tay during the period analyzed. Ten keywords in English and Spanish were employed to find the news in media's search engines: Tay, *Inteligencia Artificial*, Artificial Intelligence, AI, *IA*, Bot, Chat Bot, Microsoft, digital assistant, *asistente digital*. 56 news stories were finally collected from thirteen international digital newspapers. Six of them in Spanish (El País, El Mundo, La Vanguardia, ABC, Eldiario.es, La Razón, and The Huffintong Post – Spain Edition), and seven of them in English (The Huffington Post - UK Edition, The Guardian, The New York Times - International Edition, The Verge, Wired and ZD Net).

From the methodological point of view, our approach is deductive. A first reading of the news shows us that the media was likely to have adopted primarily or exclusively an approach focused on attribution of responsibility and conflict. Moreover, Tay's event is a political issue (it raises concerns on Nazism, racism, homophobia or sexism and involves questions regarding the limits of freedom of expression, or the regulation of big data and artificial intelligence technologies), and it is a case of crisis communication. On this basis, the objective of the analysis is to quantify the presence of the five frames defined by Semetko and Valkenburg (2000) in the media coverage of Tay.

The sample of news stories, then, was categorized by three different coders by means of Semetko and Valkenburg's classification (Krippendorff's alpha = 0.91), focusing on the way media outlets attributed the responsibility of Tay's failure and turning into a misogynist and racist chatbot. We also coded the actors involved in the event, the causes of the failure and its responsible, the consequences and the actors that were affected by these consequences.

Concurring with Semetko and Valkenburg (2000)'s study, the results of the framing analysis revealed that the attribution of responsibility was the main frame (one out of two news stories) used by media in depicting Tay's failure. This frame was complemented by the conflict frame in 8 out of 56 cases (14%). The third most used frame was that of human interest, while none of the news stories analysed used the frames of economic consequences or morality.

Framing and content analysis show that the event was depicted to shape public understanding about who is to be blamed for Tay's malfunctioning. Media outlets tended to represent the event through the following pattern: Twitter users (the agent) maliciously misused and attacked (causal contribution) a feeble and vulnerable chatbot called Tay (the patient) that had to be disconnected by its designer (consequence).

Results show that almost three out of four stories were focused on trying to identify the culprits of Tay's malfunctioning. A third of the news stories described an orchestrated attack from Twitter users, which abused Tay and led it to behave in an inappropriate manner as the cause of the event. Precisely Twitter users were identified in 40% of the news as the actor responsible (agent) of the incident, while only a 17% do it with Microsoft. On the other hand, 18% of the news reported the interaction between humans and Tay's software as the trigger of the fiasco, while 14% of the stories described the malfunctioning as a failure of Tay's machine-learning code.

The consequences reported were the following: in one out of three news stories, the consequence reported was the disconnection of Tay and the apologies given by Microsoft. By doing so, media assume the retrospective approach to attribution of responsibility as the only possible. One out of four stories (25%) reported that the main consequence of the failure was that Tay had become a mirror of the worst of humanity by "learning" how to be racist and misogynistic. Conversely, norms and risks were not relevant in media depictions of Tay's failure. By describing the action as an attack, and clearly identifying

responsible and affected actors, media outlets stressed the existence of a conflict between Twitter users and the chatbot. Besides this, news stories are emotionally charged by depicting Tay as a person and making sensitive judgements about it.

Media tend to present the chatbot as the most affected actor (patient) in the event. A third of the news stories (33%) referred to Tay as a human being and a "baby robot" harmed by the abusers. Additionally, 9% of the stories pointed at AI as the one affected by the failure, and 5% of them at Microsoft. To sum up, the chatbot, its technology, and even its designers were presented as those ill affected by Tay's malfunctioning. Surprisingly, only 12% of the news stories considered ethnic and religious vulnerable social groups (such as black people or the Jewish community) and women offended by Tay's messages as those harmed by the incident. Finally, 9% of the stories points at Twitter users and humans in general as the injured party. There was no explicit reference to hate speech and its consequences over people, nor to legal issues.

Tay's event: the media deconstruction of reality

Media representation of Tay's event depicts a biased and misleading reality that concurs with the traditional mainstream media discourse on new technologies defined by Stahl (1995): it tends to stabilize and close the discourse of Microsoft. By presenting the event as an isolated phenomenon from any context, media do not contribute to people's media and technology literacy, nor to their social empowerment. Content and framing analysis of news showed a contradictory discourse: on the one hand, media personalized Tay and treated it as something capable to feel and suffer. On the other hand, Twitter users are dehumanized and found guilty on Tay's turn into a misogynistic and racist being. Media discourse, then, reinforces the idea that Tay failed because of Twitter users. Media referred to a retrospective accountability action performed by Microsoft (apologize) and, by assuming company's discourse, depicted a reality that favored AI business' —and particularly Microsoft's— interests. They give voice and credibility to the company, which, far from being affected, gains visibility and come out reinforced by positioning its discourse in the public sphere. In that regard, it should be noted that Tay's event coincided with the celebration of Build 2016, the annual congress of Microsoft Corporation. Consequently, 21% of news stories replicate literal ideas pronounced by Satya Nadella (CEO of Microsoft) in his opening speech at the Build 2016, about the future of artificial intelligence and his company's plans on chatbots. The most repeated one is the following: "We want to build technology that gets the best of humanity and not the worst". Likewise, the content analysis revealed that the most of the news explain the cause of the event as an orchestrated attack, an idea exposed by Peter Lee (March 25th, 2016) (Microsoft Healthcare's Corporate Vice President) in an official statement: "Unfortunately, in the first 24 hours of coming online, a coordinated attack by a subset of people exploited a vulnerability in Tay." On doing so, media repeats a discourse that goes in the best interests of Microsoft: to dwell on a conventional-retrospective approach to the responsibility of Tay's case, instead of a prospective one, while they blame Twitter users for it and present the fiasco as an isolated event.

There is a huge academic controversy among scholars in relation to the attribution of responsibility in algorithmically-controlled environments. Designers, users or both (when interacting) have been proposed as the presumed responsible for the punishable crimes committed by algorithms. However, media outlets were inclined to blame just one of the actors involved: the users. Users can be considered as instigators of

Tay's wrongdoings. They drove the chatbot to deal with specific issues, vocabulary and tone. In this sense, users persuaded Tay to be misogynistic and racist. However, this cannot be considered as the unique cause of Tay's failure. The issue stems from the fact that the algorithm was not properly designed to handle such a situation (Sandvig et al., 2016), although it seemed to be designed to simply replicate its interlocutors tone and vocabulary. As a non-rationale machine, Tay did not have the capacity of understanding what is right or wrong, but designers should have been aware of the potential harms of such a design. As noted by Diakopoulos and Friedler (2016), some a priori values should have been programmed in order to prevent the fiasco.

A remark has to be added in relation to hate speech and the attribution of responsibility. Hate speech increases social inequality, violate sensitivities and impose the domination of social groups over stigmatised others, but it could even drive the victims to fatal consequences (Zollo & Loos, 2017). Research has shown that hate speech and extremist ideologies are flourishing on the digital space because of the far-right media manipulation and spread of disinformation (Marwick & Lewis 2017, Matamoros-Fernández, 2017). Hate groups, bots, trolls and the dynamics of social networks are some of the main contributors to this phenomenon. Due to the seriousness of hate speech's social implications, it is everyone's responsibility to help eradicating it. Consequently, it makes no difference whether the messages that Twitter users actually addressed to Tay had a purpose (attack, persuade, play) or not. Users were responsible for their own messages and they should account for them, although not for those of Tay.

As pointed out by Karppi and Crawford's (2016) the failure of a computational system is an opportunity to gain knowledge about it and its social consequences. In this sense, Tay's malfunctioning must lead society to reflect on the potential harms of automated bots' behaviors, and to make clear the different responsibilities that have to be assumed by social actors, including users, designers and the owners of the platforms in which robots perform their actions. We must be specially concerned about the rise of hate speech and other unacceptable attitudes and behaviors, and force designers to prevent their algorithms from turning into Nazi, misogynistic and racist abusers. Finally, media depictions of algorithms' failures should include the complexities of algorithmically-controlled environments and foster the public debate about who is responsible for what.

Conclusions

Digital environments and, in particular, social networks have driven technology companies to design algorithms that make use of social big data and machine learning strategies to interact with a myriad of users (Neff & Nagy, 2016; Ferrara et al., 2016). However, algorithms such as those used by chatbots are playing a role in public life, so the responsibility for their actions must be taken by someone. Chatbots' very nature challenges traditional notions of responsibility and accountability. On the one hand, they lack of intentionality and agency, which are conceived as human capacities. On the other hand, randomness, complexity and opacity are well-known characteristics of the algorithms that rule chatbots. These characteristics pose a difficulty in the identification of causes and consequences of chatbots' behavior and in the attribution of responsibility for their actions in case of failure.

From a theoretical perspective, we have observed that two basic approaches to the concepts of attribution of responsibility and accountability stand out: the structuralist (Johnson; 2006) and the context-dependent

(Kroes & Verbeek, 2014). However, our exploratory research has shown that media discourse on Tay's failure was, in general, simplistic, non-critical and misleading. Although the main frame used by media to depict the event was this of the attribution of responsibility (Semetko & Valkenburg, 2000), the responsibility of Tay's conversion into a Nazi and misogynistic chatbot was attributed to Twitter users, who were described as abusers that took advantage of the machine-learning algorithms leaging its actions. Far from a structuralist or contextual approach, Tay was treated as a human entity, while users were, in general, vilified and dehumanized. This fact leads us to conclude that media depiction of Tay's event was highly biased, and that it reproduced the dominant discourse about technology, algorithms and chatbots. Media adopted Microsoft discourse by stressing that it was Tay and the company itself the ones affected by users' unappropriate interaction with the chatbot. In sum, media contribute to the construction of a friendly and neutral image of AI technology, with no responsibility to be held.

Finally, media and other social institutions should put pressure on tech companies and denounce the undesirable consequences of the opacity of their algorithms as well as to push them to be accountable for the actions performed by their artifacts. As both our theoretical review and frame analysis reveal, there is a huge controversy about who is to be blamed by machine-learning algorithms misfunctioning. Media should contribute to the debate by publishing critical approaches and explaining to their audiences how complex attributing responsibility is in an algorithmically controlled environment. In addition, the sociotechnical system where bots function and interact should also be made comprehensible.

Considering the complexity of social bots' outputs formation, there are, at least, two main ideas related to responsibility and accountability that should be transmitted by the media in cases such as Tay's. Firstly, while the responsibility for the bot's behavior belongs to the whole environment involved in bots' development and functioning, the accountability belongs only to those involved in its development and design. That is, on the part of responsibility: developers, designers (including those who decide bots' type of learning and the environment in which it is inserted); those interacting with the bot, the interaction and the environment itself. On the part of accountability, developers, designers and those who lead the process of insertion of the bot. Secondly, it seems necessary to stress the social role of responsibility as a way to balance powers and not only to blame culprits. This line implies to stress not only on the retrospective notion of accountability and responsibility, but on the prospective one, as a path for creating suitable conditions for the development of new technologies and preventing undesirable future outputs.

References

An, S-K. and Gower, K.K. (2009). How do the news media frame crises? A content analysis of crisis news coverage, *Public Relations Review,* 35, 107-112. doi: doi:10.1016/j.pubrev.2009.01.010.

Asaro, P. M. (2012). A body to kick, but still no soul to damn: Legal perspectives on robotics. In P. Lin, K. Abney, & G. A. Bekey (Eds.), *Robot ethics: The ethical and social implications of robotics*. Cambridge: MIT Press.

Baldi, V. (2017). Beyond the algorithmic and automated society. Towards a critical reappropriation of digital culture. *Observatorio (OBS),* 11(3), 186-198. doi: 1646-5954/ERC123483/2017.

Baruh, L. and Popescu, M. (2015). Big data analytics and the limits of privacy self-management. *New Media & Society,* 19(4), 1-18. doi: 10.1177/1461444815614001.

Bostrom, N. (2015). *What happens when our computers get smarter than we are?* Conference at TED Talks. https://www.ted.com/talks/nick_bostrom_what_happens_when_our_computers_get_smarter_than_we_are?language=en.

Bovens, M. (2005). Public accountability. In E. Ferlie, L. E. Lynn, & C. Pollitt (Eds.), *Oxford handbook of public management*, pp. 182–208. New York: Oxford University Press.

Boyd, D. and Crawford, K. (2011). Six provocations for big data, *Paper presented at: A decade in internet time: Symposium on the dynamics of the internet and society*. doi: http://dx.doi.org/10.2139/ssrn.1926431.

Boyd, D., and Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer Mediated Communication*, 13(1), 210–230. doi: 10.1111/j.1083-6101.2007.00393.x

Boyd, D., Levy, K. and Marwick, A. (2014). The networked nature of algorithmic discrimination. In S. Gangadharan (Ed.) *Data and discrimination: Collected essays*, 53-57. Washington, DC: Open Technology Institute – New America Foundation.

Campbell, P. (2010). Boundaries and risk: Media framing of assisted reproductive technologies and older mothers. *Social Science & Medicine*, 72, 265-272. doi:10.1016/j.socscimed.2010.10.028.

Caplan, R. and Boyd, D. (2016). Who controls the public sphere in an era of algorithms? Mediation, automation, power, *Contemporary Issues and Concerns Primer, Data & Society*. Retrieved from: https://datasociety.net/events/who-controls-public-sphere.

Carbonell, J. G., Michalski, R. S. and Mitchell, T. M. (1984). An overview of Machine Learning. An Artificial Intelligence Approach. Berlin: Springer-Verlag.

Castells, M. (2009). The Rise of the Network Society: The Information Age: Economy, Society, and Culture. Cambridge: Blackwell Publishers.

Chakrabarti, C. and Luger, G. F. (2015). Artificial conversations for customer service chatter bots: Architecture, algorithms, and evaluation metrics. *Expert Systems with Applications,* 42, 6878-6897. doi: 10.1016/j.eswa.2015.04.067.

Coman, C.& Cmeciu, C. (2014). Framing Chevron Protests in National and International Press. *Procedia - Social and Behavioral Sciences,* 149, 228 – 232.

Diakopoulos, N., and Friedler, S. (2016). How to Hold Algorithms Accountable, *MIT Technology Review, November 2016*. Retrieved from: https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/?utm_content=buffer19bc5andutm_medium=socialandutm_source=twitter.c%E2%80%A6.

Druckman, J.N. & Bolsen, T. (2011). Framing, Motivated Reasoning, and Opinions about Emergent Technologies. *International Journal of Communication, 61*: 659-688. doi:10.1111/j.1460-2466.2011.01562.x.

Entman, R. M. (1993). Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication 43*(4): 58-67. doi: https://doi.org/10.1111/j.1460-2466.1993.tb01304.x.

Ferrara, E. Varol, O. Davis, C. Menczer, F. & Flammini, A. (2016). The Rise of Social Bots. *Communications of the ACM,* 59(7), pp. 96-104. doi: 10.1145/2818717.

Fisher, J.M. (1999). Recent work on moral responsibility. *Ethics,* 110(1), 93–139.

Floridi, L. (2014). Artificial Agents and Their Moral Nature. In Kroes, P. & Verbeek, P. (Eds.), *The Moral Status of Technical Artefacts, 17*: 185-212. Springer Dordrecht Heidelberg, New York, London.

Floridi, L. and Sanders, J. (2004). On the morality of artificial agents, *Minds and Machines, (14)*3, pp: 349. doi: https://doi-org.sare.upf.edu/10.1023/B:MIND.0000035461.63578.9d.

Ford, H.R, Dubois, E. & Puschmann, C. (2016). "Keeping Ottawa Honest—One Tweet at a Time? Politicians, Journalists, Wikipedians, and Their Twitter Bots". *International Journal of Communication, 10*: 4891-4914. doi: 1932–8036/20160005.

Gamson, W. A. (1992). *Talking politics*. New York: Cambridge University Press.

Gotterbarn D. (2001). "Informatics and professional responsibility,". *Science and Engineering Ethics, 7*(2): 221–230.

Griol, D., Sanchis de Miguel, A. and Molina, J. M. (2014). 'Giving Voice to the Internet by Means of Conversational Agents'. In Corchado E., Lozano J.A., Quintián H., Yin H. (Eds). *Intelligent Data Engineering and Automated Learning*. doi: 10.1007/978-3-319-10840-7_53.

Groom, V., Chen, J., Johnson, T., Kara, F. A. and Nass, C. (2010). Critic, Compatriot, or Chump?: Responses to Robot Blame Attribution, *Proceedings of the 5th ACM/IEEE International Conference on Human-Robot Interaction , March 02-05, 2010, Osaka, Japan*. doi: 978-1-4244-4893-7.

Guilbeault, D. (2016). "Growing Bot Security: An Ecological View of Bot Agency". *International Journal of Communication, 10*: 5003-5021. doi: 1932–8036/20160005.

Hallinan, B. and Striphas, T. (2016). Recommended for you: The Netflix Prize and the production of algorithmic culture. *New Media and Society, 18*(1): 117-137. doi: 10.1177/1461444814538646.

Hellström, T. (2013). On the moral responsibility of military robots. *Ethics and Information Technology, 12*(2): 99-107.

Introna, L. D. (2014). 'Towards a Post-human Intra-actional Account of Sociomaterial Agency (and Morality)'. In Peter Kroes & Peter-Paul Verbeek (Eds.), *The Moral Status of Technical Artefacts:* 31-53. New York, London: Springer.

Johnson, D. G. (2006). Computer Systems: Moral Entities but not Moral Agents. *Ethics and Information Technology, 8*, pp: 195–204.

Karppi, T., and Crawford, K. (2016). Social Media, Financial Algorithms and the Hack Crash. *Theory, Culture and Society, 33*(1), 73-92. doi: 10.1177/0263276415583139.

Kemper, J. and Kolkman, D. (2018). Transparent to whom? No algorithmic accountability without a critical audience. *Information, Communication & Society,* doi: 10.1080/1369118X.2018.1477967.

Kollani, B., Howard, P. and Wooley, S. C. (2016). Bots and Automation over Twitter during the Third U.S. Presidential Debate, *Data Memo 2016.3. Oxford, UK: Project on Computational Propaganda*. https://www.oii.ox.ac.uk/blog/bots-and-automation-over-twitter-during-the-third-u-s-presidential-debate/.

Kroes, P., and Verbeek, P-P. (2014). *The Moral Status of Technical Artefacts*. New York, London: Springer.

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., and Yu, H. (2017). Accountable algorithms, *University of Pennsylvania Law Review*, 165: 633. Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/pnlr165&div=20&id=&page=&t=1558886997.

Laney, D. (2001). 3D data management: Controlling data, volume, velocity and variety, *Application delivery strategies*, *File 949.* Meta Group Research Note. Retrieved from: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Lawrence, R. G. (2000). Game-Framing the Issues: Tracking the Strategy Frame in Public Policy News, *Political Communication*. doi: 10.1080/105846000198422.

LeCun, Y., Bengio, Y. and Hinton, G. (2015). Review. Deep Learning. *Nature, 521*: 436-444. doi: 10.1038/nature14539.

Lee, P. (March, 25th 2016). *Learning from Tay's introduction*, Statement published in The Official Microsoft Blog. Retrieved from: https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/.

Lesk, M. (1997). *How Much Information Is There In the World?* Retrieved from: http://www.lesk.com/mlesk/ksg97/ksg.html.

Marechal, N. (2016). "When Bots Tweet: Toward a Normative Framework for Bots on Social Networking Sites". *International Journal of Communication, 10*: 5022-5031. doi: 1932–8036/2016FEA0002.

Marsland, S. (2015*). Machine Learning: An Algorithmic Perspective.* Boca Raton: CRC Press.

Marwick, A. and Lewis, R. (2017). *Media Manipulation and Disinformation Online*, New York: Data & Society Research Institute. Retrieved from: https://datasociety.net/output/media-manipulation-and-disinfo-online/.

Matamoros-Fernández, A. (2017). Platformed Racism: The Mediation and Circulation of an Australian Race-Based Controversy on Twitter, Facebook and YouTube. *Information Communication and Society*, 20 (6), 930–46. doi:10.1080/1369118X.2017.1293130.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology, 6*(3): 175-183.

Microsoft Corporation. (2016). *Tay.ai Official Webpage* [now disabled]. Retrieved from: www.tay.ai.

Mitcham, C. (2014). 'Agency in humans and in artifacts: A contested discourse'. In Kroes, P. and Verbeek, P_P. (Eds.), *The moral status of technical artifacts*: 11-29. Dordrecht, The Netherlands: Springer Science and Business Media. doi: 10.1007/978-94-007-7914-3_2.

Murthy, D., Powell, A. B., Tinati, R., Anstead, N., Carr, L., Halford, S.J., and Weal, Mark (2016). Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital*. International Journal of Communication*, 10: 4952-4971. doi: 1932–8036/20160005.

Nath, V. and Levinson, S.E. (2014). *Autonomous robotics and Deep Learning.* New York, London: Springer.

Neff, G. and Nagy, P. (2016). Talking to Bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication, 10*, 4915-4931. doi: 1932–8036/20160005.

Nichols, N. (2010). Machine-Generated Content: Creating Compelling New Content from Existing Online Sources. Ph.D. Dissertation. Northwestern University, Evanston, IL, USA.

Olsher, D. (2014). Semantically-based priors and nuanced knowledge core for Big Data, Social AI, and language understanding. *Neural Networks, 58:* 131-147. doi: 10.1016/j.neunet.2014.05.022.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Puschmann, C. and Burgess, J. (2014). Metaphors of Big Data. *International Journal of Communication*, 8: 1690–1709. http://ijoc.org/index.php/ijoc/article/view/2169.

Rieder, B. (2018). Beyond Surveillance: How Do Markets and Algorithms 'Think'? *Le foucaldien*, 3(1) 8, pp. 1–20, DOI: https://doi.org/10.16995/lefou.30.

Rieder, B., Matamoros-Fernández, A., and Coromina, Ò. (2018). From ranking algorithms to 'ranking cultures': Investigating the modulation of visibility in YouTube search results. *Convergence*, 24(1), 50–68. http://doi.org/10.1177/1354856517736982.

Rosenblat, A., Kneese, T. and boyd, d. (2014). Algorithmic Accountability, *The Social, Cultural & Ethical Dimensions of "Big Data"*. doi: http://dx.doi.org/10.2139/ssrn.2535540.

Sandvig, Ch., Hamilton, K., Karahalios, K., and Langbort, C. (2016). When the Algorithm Itself Is a Racist: Diagnosing Ethical Harm in the Basic Components of Software. *International Journal of Communication, 10*: 4972-4990. doi: 1932–8036/20160005.

Semetko, H. a., and Valkenburg, P. M. (2000). Framing European Politics. A Content Analysis of Press and Television News. *Journal of Communication*, *50:* 93-1009. doi: 10.1111/j.1460-2466.2000.tb02843.x.

Shalev-Shwartz, S. and Ben-David, S. (2014*). Understanding Machine Learning: From theory to Algorithms*. New York: Cambridge University Press.

Spicer, A. (2005). The political process of inscribing a new technology. *Human Relations, 58*(7): 867-890. doi: 10.1177/0018726705057809

Stahl, W.A. (1995). Venerating the Black Box: Magic in Media Discourse on Technology. *Science, Technology and Human Values, 20*(2): 234-258. http://www.jstor.org/stable/689992.

Suárez-Gonzalo, Sara (2017). Big Social Data: some limitations of Notice and Choice for privacy protection. *El profesional de la información, 26*(2), pp. 283-292. doi: 10.3145/epi.2017.mar.15

Tufekci, Z. (2014). Big questions for social media big data: Representativeness, validity and other methodological pitfalls. *Procedings of the 8th Intl AAAI Conferece on weblogs and social media.* https://arxiv.org/abs/1403.7400.

van Dijk, J. (2013). *The cutlure of connectivity. A critical history of social media*. New York: Oxford University Press.

Waelbers, K. (2009). Technological Delegation: Responsibility for the Unintended. *Science & Engineering Ethics, 15*(1): 51–68.

Zollo, S. A. and Loos, E. (2017). No Hate Speech Movement: evolving genres and discourses in the European online campaign to fight discrimination and racism. *Observatorio, 11*(2): 91-107. doi: 1646-5954/ERC123483/2017.

3

Suárez-Gonzalo, Sara (2017). Big social data: límites del modelo *notice and choice* para la protección de la privacidad, *El profesional de la información, 26*(2): 283-292. doi: https://doi.org/10.3145/epi.2017.mar.15.

ISSN: 1386-6710. ISSN electrónico: 1699-2407.

BIG SOCIAL DATA: LÍMITES DEL MODELO *NOTICE AND CHOICE* PARA LA PROTECCIÓN DE LA PRIVACIDAD

Big social data: Some limitations of *notice and choice* for privacy protection

Sara Suárez-Gonzalo

Sara Suárez-Gonzalo lleva a cabo su tesis doctoral en el *Departament de Comunicació* de la *Universitat Pompeu Fabra*. Se graduó en Publicidad y Relaciones Públicas por la *Universidade de Vigo* en 2014 y master en *Comunicación Social* por la *Universitat Pompeu Fabra* en 2015. Desde 2014 investiga el impacto del fenómeno *big data* en la privacidad de las personas, especialmente en las redes sociales.
http://orcid.org/0000-0001-6883-1984

Universitat Pompeu Fabra. Departament de Comunicació
Programa de doctorado
Roc Boronat, 138, 08018 Barcelona, España
sarapaz.suarez@upf.edu

Resumen

El fenómeno *big data* supone un desafío a la privacidad de los datos personales (Boyd, 2012). Este artículo es una contribución al debate sobre la validez del paradigma de autogestión de la privacidad reinante en el mundo occidental. Se señalan una serie de limitaciones del modelo en el que se basa dicho paradigma (el modelo *notice and choice*) con respecto a la lógica de procesamiento *big data*. También se analiza el modelo alternativo propuesto por Solove (2013) para explicar por qué no se aleja en lo esencial del modelo *notice and choice*. Por último, se expone la necesidad de construir un modelo cuya fundamendación conceptual sea coherente con la lógica *big data* y su impacto en la privacidad a nivel individual y colectivo.

Palabras clave

Big data; Datos masivos; Autogestión de la privacidad; *Notice and choice*; Libertad; Privacidad colectiva; Protección de datos personales; Ética; Solove; Paradoja de la privacidad; Redes sociales.

Abstract

Big data challenges personal data protection (Boyd, 2012). This paper is a contribution to the debate about the validity of the privacy self-management paradigm prevailing in western countries. I point out some limitations of the model *notice and choice* in which that paradigm is based in relation to the logic of big data processing. I also analyze the alternative model proposed by Solove (2013), to explain why it is not essentially different from *notice and choice* model. Finally, I expound on the necessity of developing a model which could be coherent with the logic of big data and its impact in privacy, both individual and collective.

Keywords

Big data; Privacy self-management; *Notice and choice*; Freedom; Liberty; Collective privacy; Personal data protection; Ethics; Solove; Privacy paradox; Social networks.

Suárez-Gonzalo, Sara (2017). "*Big social data*: límites del modelo *notice and choice* para la protección de la privacidad". *El profesional de la información*, v. 26, n. 2, pp. 283-292.

https://doi.org/10.3145/epi.2017.mar.15

Artículo recibido el 11-11-2016
Aceptación definitiva: 24-01-2017

1. Introducción

La "datificación" de lo cotidiano es una tendencia en alza (**Baruh**; **Popescu**, 2015, p. 3). A finales del siglo XX el volumen, la variedad y la velocidad de generación de datos comenzó a aumentar notablemente (**Laney**, 2001) y surgió el término *big data* (**Cox**; **Ellsworth**, 1997, p. 1). Hoy numerosas actividades del mundo digital y del presencial se registran en datos, que gracias al desarrollo tecnológico pueden recopilarse de forma rápida y barata (**Halavais**, 2015), siendo su usabilidad cada vez mejor (**Minelli**; **Chambers**; **Dhiraj**, 2013). Como consecuencia aumenta el número y la variedad de sectores interesados en los datos masivos (**Chen**; **Zhang**, 2014), al tiempo que crece la preocupación social por la privacidad, un concepto complejo que recogen como derecho fundamental numerosas constituciones (**Solove**, 2008). Sin embargo, varios estudios muestran que a menudo los comportamientos de las personas con respecto a la difusión de su información personal no reflejan esa preocupación (**Durán-Segura**; **Mejías-Peligro**, 2014; **Hargittai**; **Marwik**, 2016; **Hoy**; **Milne**, 2013; **Solove**, 2013; **Taddicken**, 2014; **Utz**; **Kramer**, 2009), dando lugar a la llamada "paradoja de la privacidad" (**Barnes**, 2006). **Barnes** atribuye esta incoherencia a las características personales de los individuos, pero **Turow**, **Hennessy** y **Draper** (2015) sugieren que se trata de una imposibilidad de los individuos para decidir acerca de su privacidad. Más allá de esto, la "paradoja del conocimiento" (**Baruh**; **Popescu**, 2015, p. 9) describe la posición de individuos muy informados y concienciados que, frente a la imposibilidad de proteger sus datos, rechazan la tecnología como una táctica de resistencia. Algunos tienden al *suicidio digital* (**Karppi**, 2011; **Dockray**, 2010).

El fenómeno *big data* supone un problema social para la protección de los datos personales y un desafío para la ordenación jurídica en materia de privacidad (**Jourová**, 2016). En el mundo occidental la legislación sobre privacidad de los datos personales sigue el modelo de la autogestión (*privacy self-managment*), que se basa en la notificación y la elección (*notice and choice*) (**Baruh**; **Popescu**, 2015; **Schwartz**, 2013; **Solove**, 2013). En la práctica, la información proporcionada a los individuos sobre el uso de sus datos es larga y compleja y no se produce una negociación (**Solove**, 2013). En la mayoría de los casos el consentimiento se rige por la máxima "lo tomas o lo dejas" (**Popescu**; **Baruh**, 2013). En el entorno académico emerge un debate sobre la conveniencia y las limitaciones de la autogestión (**Baruh**; **Popescu**, 2015; **Martin**, 2015; **Schwartz**, 2013; **Solove**, 2008; 2013), y este artículo es una contribución al mismo. El objetivo es identificar algunos de los factores que obstaculizan la protección de la privacidad de los datos personales mediante los mecanismos de la notificación y la elección en un mundo tecnológico profundamente interconectado.

2. Privacidad y lógica *big data*

2.1. La difusión de información personal

Los usuarios ceden una gran cantidad de información personal en las redes sociales, cimentando un rastro indisoluble (**Burkell** *et al.*, 2014; **Manovich**, 2012). Como explican **Boyd** y **Crawford** (2011), en ellas los usuarios cambian la forma tradicional de compartir información, y como consecuencia cada vez están más expuestos.

Estos datos masivos (conocidos en inglés como *big social data*, *social media data o social media big data*, **Tufekci**, 2014, **Halavais**, 2015, p. 586) despiertan un gran interés a las empresas y ya están siendo utilizados para incrementar la inteligencia de mercado (**He** *et al.*, 2015), en la predicción y gestión de situaciones de crisis y emergencia (**Castillo**, 2016; **Xiao**; **Huang**; **Wu**, 2015; **Pohl**; **Bouchachia**; **Hellwagner**, 2015), y también para mejorar tratamientos médicos (**Sarker** *et al.*, 2015; **Gouveia-Rodrigues** *et al.*, 2014), entre otras aplicaciones.

En ocasiones la difusión de información personal es consciente, en otras no. Las aplicaciones generan metadatos de forma automática que pueden revelar la localización, el tiempo o características del dispositivo desde el que se genera la información, tanto del individuo principal, como de aquellos con los que éste se comunica (*Privacy International*, s.f.). Asimismo, la información personal que genera y difunde una persona también la difunden otros. Es decir, la difusión de información personal no es sólo personal.

> "La difusión de información personal no es algo personal"

2.2. Procesamiento *big data*

Una característica de la recogida de datos masivos es que es indiscriminada. En los métodos tradicionales antes de recopilar se decide qué datos interesan, pero en la minería *big data* de entrada se obtiene un conjunto completo de información al que posteriormente se aplican filtros (**Baruh**; **Popescu**, 2015) y se cruzan las variables (**Solove**, 2013; **Baruh**; **Popescu**, 2015) con el objetivo de extraer información valiosa no explícita, una información que emerge combinando los datos. Esto permite estudiar fenómenos a gran escala (**Halavais**, 2015), vislumbrar atributos y patrones latentes en los datos (**Boyd**; **Crawford**, 2011) e inferir información que las personas no han difundido de forma explícita (**Tufekci**, 2015). En consecuencia, datos que de forma aislada parecen inocuos, procesados pueden revelar información sensible.

Facebook for business (2014) declara que el propósito del análisis de datos masivos no es vigilar la actividad individual, sino extraer información valiosa del conjunto de las expresiones colectivas. En este sentido, no sólo se recoge información detallada de los hábitos y preferencias de millones de personas (que permitiría vigilarlas individualmente si este fuera el objetivo), sino que sirve para estudiar los patrones de comportamiento y actuación de conjuntos más amplios de la sociedad. En publicidad esto permite adecuar productos y servicios, realizar campañas publicitarias más efectivas o predecir comportamientos o actitudes futuras de los consumidores (**Mayer-Schönberger**; **Cukier**, 2013; **Schroeck** *et al.*, 2012). El éxito de plataformas como *Amazon* o *Netflix* se debe en gran medida al uso de sistemas de recomendación automatizados basados en la similitud entre usuarios (**Capella**; **Yang**; **Lee**, 2015; **Fernández-Manzano**; **Neira**; **Clares-Gavilán**, 2016).

2.3. Automatismo y opacidad

Los procesos *big data* afectan directa o indirectamente a la vida de las personas (**Kroll** *et al.*, 2016), con aplicaciones tan importantes como la negociación de alta frecuencia de los mercados financieros (**Karppi**; **Crawford**, 2016, p. 2) o la persecución del crimen (**Bogomolov** *et al.*, 2014; **DeLorenzi**; **Shane**; **Amendola**, 2006). Hallinan y Striphas definen la cultura algorítmica como el uso de procesos computacionales para ordenar, clasificar y jerarquizar personas, lugares, objetos, y también los hábitos de pensamiento, conducta y expresión que emergen en relación con estos procesos (**Hallinan**; **Striphas**, 2016, p. 119). Al mismo tiempo que se hacen más complejos, explica **Pasquale** (2015), estos sistemas de procesamiento se vuelven cada vez más opacos debido al interés de los grandes poderes corporativos y gubernamentales, al amparo de los sistemas políticos y legales. Pasquale utiliza el término *agnotology* para referirse a la producción estructural de ignorancia, sus diversas causas y conformaciones, tanto si se deben a la negligencia, despiste, miopía, extinción, secretismo o la ocultación (**Pasquale**, 2015, p. 2). Este escenario despierta reclamos de transparencia, responsabilidad y control de los procesos de análisis de datos, a los que se suman muchos expertos por motivos diversos:

- **Capland** y **Boyd** (2016) defienden que los algoritmos están modificando la esfera pública;
- **Boyd**, **Levy** y **Marwik** (2014) señalan sus posibles efectos discriminatorios;
- **Pasquale** (2015) y **Kroll** *et al.* (2016) apuntan que carecen de la objetividad y la neutralidad de la que presumen.

Al mismo tiempo se extiende la convicción de que la mera transparencia no es suficiente para hacer frente a esta situación. Varios autores, entre ellos **Pasquale** (2015) o **Boyd** (2016), defienden que, por sí sola, la transparencia puede conducir simplemente a más complejidad y que, por ello, existe una necesidad de establecer procesos de control y atribución de responsabilidades.

> “La violación de la privacidad adquiere una dimensión colectiva”

2.4. Violación de la privacidad

La protección de la privacidad de los datos personales en este escenario es, cuanto menos, compleja:

- la difusión de datos personales no es algo personal ni controlable por la persona a la que pertenecen;
- los mecanismos a los que se someten dichos datos no son comprensibles ni transparentes y carecen de responsabilidad directa y de control externo.

Así, la violación de la privacidad puede ser imprevisible, puede producirse a largo término y no sólo se ocasiona a nivel individual, sino que adquiere una dimensión colectiva y afecta al conjunto de la sociedad.

3. Autogestión de la privacidad en el mundo occidental

Las leyes de protección de la privacidad de datos personales en el mundo occidental son similares (**Metcalf**; **Crawford**, 2016): comparten el paradigma de autogestión de la privacidad (**Schwartz**, 2013), que se basa en el modelo *notice and choice* (**Solove**, 2013; **Baruh**; **Popescu**, 2015).

Seguidamente se explican algunas características principales de la legislación europea y la estadounidense en la materia con el fin de mostrar que comparten unas características esenciales e ilustrar la plasmación jurídica del modelo *notice and choice*. Es importante destacar que el presente artículo se centra en este modelo como el ente abstracto que reúne las características esenciales del paradigma de protección de la privacidad de datos personales predominante en el mundo occidental.

Las leyes de protección de datos personales de Europa y Estados Unidos tienen su origen en las *Fair information practices* de 1973, una serie de principios básicos compartidos entre Estados Unidos y Europa occidental para las organizaciones del sector público y privado que procesaran información personal (**Schwartz**, 2013; **Solove**, 2013). Como indica **Schwartz** (2013), existen diferencias entre los reglamentos europeo y estadounidense que se han acentuado con la entrada en vigor en abril de 2016 del *Reglamento 2016/679 del Parlamento Europeo y del Consejo* (*Unión Europea*, 2016), más rígido en la protección de datos personales con respecto a la ya derogada *Directiva* de 1995 (*Unión Europea*, 1995). **Jourová** (2016) señala que esta reforma del *Reglamento* se centra en tres aspectos principales:

- resguardar el derecho fundamental a la protección de datos independientemente de cómo se desenvuelvan en el futuro la tecnología y el entorno digital;
- aumentar la confianza en el entorno digital;
- incrementar la actividad económica.

Como diferencias principales, la legislación europea establece reglas generales y unificadas para todos los estados miembros de la Unión. A mayores, una legislación sectorial se encarga de especificar las normas para casos concretos. Por el contrario la estadounidense es sectorial y establece diferentes estatutos para el ámbito público y el privado (**Schwartz**, 2013, p. 1974).

La regulación europea establece unos límites más estrictos que la estadounidense para la recopilación y el uso de datos, da protección adicional a aquellos de carácter sensible y defiende más derechos de los individuos. Asimismo, da más importancia a la notificación mediante un principio de transparencia que obliga al responsable del tratamiento de los datos a proporcionar información al afectado de que se están recogiendo, consultando o tratando datos que le conciernen, de una manera fácilmente accesible y con un lenguaje claro y sencillo. Se considera que el consentimiento es informado si el individuo conoce al menos la identidad del responsable del tratamiento de los datos y los fines para los que se recogen dichos datos. Esta regulación establece

medidas de control del consentimiento, interviene el flujo transfronterizo de datos e instaura agencias nacionales de control interno. Por su parte, la legislación estadounidense concede más importancia al consentimiento de las partes afectadas y menos a la notificación. En su caso, la *Federal Trade Commission* es el órgano más similar a una agencia nacional de control (**Schwartz**, 2013).

3.1. *Notice and choice*: condiciones básicas

Las diferencias fundamentales entre la regulación europea y la estadounidense se concentran en la forma de implementación de las normativas y en la centralidad de la notificación o el consentimiento. El reglamento europeo es más estricto con la notificación y el consentimiento y es más garantista que el estadounidense. En todo caso, su esencia es compartida: la notificación y la elección son las condiciones básicas para el funcionamiento del modelo *notice and choice* y la decisión individual la manera de proteger la privacidad.

Debido a que la regulación europea es la más exigente, se exponen como ejemplo los criterios que se extraen de su lectura al respecto de la notificación y el consentimiento:

- el consentimiento debe ser libre, informado, específico para cada caso concreto y revocable y debe reflejarse en un acto afirmativo claro e inequívoco;
- la notificación sirve de base para que el afectado dé su consentimiento de manera informada y por lo tanto debe ser previa a la recopilación o tratamiento de los datos, y cumplir las condiciones de ser adecuada e inequívoca.

> La legislación occidental en materia de datos personales sigue el paradigma de la autogestión

4. Crítica al modelo *notice and choice*

4.1. Limitaciones: lógica *big data*

Se extrae de lo anteriormente expuesto que para el funcionamiento del modelo *notice and choice* es esencial determinar de forma clara qué es un dato personal o qué datos pueden revelar información personal. Es necesario, al menos, para determinar:

- a qué individuos se proporciona la información y el derecho a consentir;
- cuándo puede surgir un problema de privacidad o un conflicto de intereses derivado del tratamiento de datos;
- sobre qué cuestiones se debe informar y consentir.

Sin embargo, lo argumentado en el apartado **2.2. Procesamiento *big data*** se traduce en una dificultad para determinar qué constituye un dato personal hoy en día, lo cual dificulta el cumplimiento de los criterios de funcionamiento del modelo *notice and choice*. En base al ejemplo europeo: la información al individuo difícilmente puede ser inequívoca y adecuada, si se proporciona previamente a la recopilación y al tratamiento de los datos. Por consiguiente difícilmente podríamos considerar que el consentimiento sea informado y que se pueda proporcionar o revocar de forma específica para cada caso.

En este artículo se considera que el cumplimiento de dichos criterios pasaría por:

- definir con claridad qué es un dato personal;
- proporcionar información completa y adecuada al individuo;
- permitir la decisión informada y significativa acerca de cualquier aspecto relativo a todas las posibles formas de tratamiento de dichos datos, en cualquier fase del proceso.

> La lógica *big data* supone una dificultad para determinar qué es un dato personal

Para que la decisión sea informada el individuo debería tener conocimiento, al menos, sobre las siguientes cuestiones:

- qué datos de los recogidos pueden concernirle, independientemente de quién los haya difundido, de cómo se hayan generado y de cómo serán procesados;
- cuáles son los objetivos, el diseño y el funcionamiento del sistema de análisis;
- qué información sensible puede revelar el conjunto de los datos analizados en cada una de las fases de análisis y, por lo tanto, de forma prolongada en el tiempo.

El cumplimiento de estos criterios complicaría en gran medida el proceso y supondría un esfuerzo desproporcionado para el individuo, no sólo por el tiempo de dedicación que requeriría, sino también por los conocimientos específicos necesarios para comprender información compleja. La información debe ser un derecho del individuo, y no una obligación para proteger los datos personales. A esto se suma la ineludible barrera que supone la intencionada opacidad de los sistemas de procesamiento de datos.

Teniendo en cuenta las limitaciones señaladas para que el consentimiento individual sea efectivamente informado y por lo tanto específico y revocable, queda por considerar el cumplimiento de un último criterio: ¿es libre?

4.2. Limitaciones: fundamentación conceptual

Para el modelo *notice and choice* "libre" equivale a "voluntario". El consentimiento se considera libre siempre que no exista una interferencia externa que afecte de forma directa a la voluntad del individuo de dar su consentimiento. Por este motivo, autores como **Richardson** (2016) han señalado que los regímenes legales occidentales de protección de datos se fundamentan en el canon tradicional de la privacidad. Éste se construye en base al ideal liberal de la libertad, como no-interferencia: para que una decisión sea libre es necesario y suficiente que no exista una interferencia en el propio curso de acción (**Berlin**, 1988, p. 196; **Hobbes**, 2011, p. 187).

Bobbio (2009, p. 98) explica dicha interferencia en términos de prohibición u obligación: la libertad consiste en la ausencia de prohibición (obligar a no hacer algo), y en la ausencia de obligación (obligar a hacer algo).

El liberalismo entiende por interferencia únicamente la intervención directa en la voluntad del individuo (**Pettit**, 2004). En el caso español esto se ve de forma clara en la *Guía para el ciudadano* que explica que el consentimiento

del individuo, recogido por la *Ley orgánica 15/1999* (*España*, 1999), debe ser libre: "salvo que la ley lo disponga no podemos ser obligados a facilitar nuestros datos" (*Agencia Española de Protección de Datos*, 2011, p. 10).

Varios autores han notado que la concepción liberal de libertad se construye sobre una idea individualista de la sociedad, que se comprende y se analiza como una suma de individuos aislados, atomizados (**Bertomeu**; **Domènech**, 2005). El liberalismo entiende, con todo, que la vida en común hace obligada la imposición de ciertas barreras a dicha libertad, a fin de garantizar que la de uno no se inmiscuya en la de otro hasta el punto de dañarla, y así, asegurar otros valores como la seguridad o la propiedad (**Mill** en **Berlin**, 1988, p. 197). Esto ayuda a comprender por qué el modelo *notice and choice* asume que garantizar la libre gestión de la privacidad pasa, justamente, por dejar que cada uno la gestione individualmente. O lo que es lo mismo: por cargar el peso de la protección de la privacidad sobre los individuos y sus decisiones. Del mismo modo se explica por qué esta norma se rompe en aquellos casos justificados por razones de orden público, como la persecución del terrorismo.

> Los fundamentos conceptuales del paradigma actual están desvinculados de la lógica y los objetivos del procesamiento de datos masivos

Desde esta perspectiva individualista, la privacidad se entiende como un espacio donde poder disfrutar de lo propio sin ser interferido (**Richardson**, 2016). Lo privado se ha identificado tradicionalmente con lo oculto, lo secreto, aquello que el individuo desea preservar del conocimiento y la acción de los demás (**Solove**, 2008). Por ello se prohíbe el acceso y la utilización de los datos personales del individuo, excepto en caso de que éste lo consienta, o de que sea él mismo quien los revele en un espacio público. Una cuestión importante, que no se abordará aquí pero que cabe apuntar, es si las redes sociales deben o no ser consideradas espacios públicos.

4.3. Choque de perspectivas

Mientras la lógica de procesamiento *big data* aprovecha el carácter interconectado de los datos y de las personas a las que pertenecen (**Boyd**, 2012) –a fin de extraer la mayor cantidad de información posible, el modelo de protección de datos personales se construye en base a una visión individualista de la sociedad, y se focaliza en los datos como entes aislados. Esta desvinculación entre las dos perspectivas pone de manifiesto una debilidad de la fundamentación conceptual del modelo *notice and choice* para comprender y abordar las vulneraciones provocadas por el uso de datos masivos.

El problema para gestionar la privacidad surge de:

- la lógica de generación y procesamiento de los datos masivos;
- un desacoplamiento entre dicha lógica y aquella de la que parte el modelo de protección de datos personales.

En la medida en que el problema afecta al conjunto de la sociedad, y cuyo control trasciende al conocimiento, las capacidades y las habilidades de cada individuo, se considera aquí un problema de tipo estructural. Atendiendo a los criterios del modelo *notice and choice*, pese a las limitaciones que supone este problema estructural para el buen funcionamiento del paradigma de autogestión, la decisión individual se seguiría considerando libre. Desde la perspectiva del presente artículo se considera que, si bien estas limitaciones no suponen una forma de interferencia directa sobre la voluntad de los individuos, sí representan otra forma de interferencia que merma la posibilidad de los individuos para gestionar sus datos personales y para hacer frente al impacto de su procesamiento. Por consiguiente se entiende que, en estas circunstancias, el consentimiento no es libre.

Como se ha dicho antes, ésta es una crítica al modelo *notice and choice* y no necesariamente a todas las formas de su plasmación jurídica. No obstante, cabe matizar que el *Reglamento* europeo recoge una idea matizada de la libertad aquí descrita, pese a que sigue remitiendo a ella (véanse las consideraciones 42 y 43 del *Reglamento*).

5. Crítica al *modelo mixto*

Una propuesta alternativa al modelo *notice and choice* es la del profesor **Solove** (2013), a la que aquí nos referimos como *modelo mixto*. Su planteamiento parte de una crítica al modelo *notice and choice* y se explica brevemente a continuación con el fin de demostrar que no se aleja en lo esencial del modelo criticado.

5.1. Puntos de divergencia

Existen tres cuestiones principales por las que, desde la perspectiva del presente artículo, el *modelo mixto* no parece adecuado:

La privacidad como valor contextual

La principal crítica de Solove al modelo *notice and choice* parte de su concepción de la privacidad. Para **Solove** (2008) la privacidad no debe conceptualizarse mediante la identificación de elementos esenciales o constitutivos de lo que ésta representa. **Solove** (2013) la entiende como un valor contextual que sólo puede conceptualizarse en relación con los daños que provoca su vulneración. Estos daños, explica, sólo pueden ser valorados en cada caso particular, es decir, en relación con el fin para el que sirva la vulneración de aquello que se considera privado. Siguiendo esta línea, Solove argumenta que el daño provocado por la vulneración de lo privado puede verse compensado en relación con otros posibles beneficios a nivel individual o social.

Esta tesis se inscribe en una forma de relativismo moral, que entiende que no es posible determinar de forma abstracta un ideal de lo que es una buena o una mala gestión de la privacidad, sino que es algo que corresponde decidir únicamente a cada individuo. Cualquier interferencia externa en esta decisión individual puede ir en contra de los intereses particulares y de la voluntad del individuo y, por lo tanto, limita la libertad y la autonomía de las personas. En consecuencia Solove considera que la gestión de la privacidad debe ser individual. Así, el *modelo mixto* conserva la premi-

sa fundamental del modelo criticado: comprende la libertad como no-interferencia, y defiende la autogestión de la privacidad como la manera de garantizar que la decisión acerca de la privacidad sea libre.

Por otra parte, el fin para el que se recojan o traten los datos (ya sea en aras del beneficio individual o colectivo, público o privado) es importante, pero no suficiente para guiar los procesos de recopilación y tratamiento de datos, ni los mecanismos de autogestión de la privacidad de datos personales. La privacidad no debe ser un mero valor contextual, ni entrar en un juego de preferencias como moneda de cambio. Debe existir algún criterio común para determinar lo que es una buena o una mala gestión de la privacidad. Las diferencias culturales deben ser tenidas en cuenta a la hora de determinar dicho criterio, comprender en qué consiste la privacidad y articular los mecanismos necesarios para protegerla.

> Determinar para qué fines es lícito tratar datos masivos y para cuáles no, es importante, pero aún lo es más asegurar que los procesos sean justos, responsables y permitan a los ciudadanos el control sobre su información

Problemas cognitivos y estructurales

Solove identifica una serie de problemas cognitivos, relativos a la falta de habilidad de los individuos para tomar decisiones racionales e informadas. Señala que los individuos, además de estar desinformados, tienen una racionalidad limitada.

Por otra parte encuentra varios problemas estructurales:

- un problema de escala, referido a un número demasiado elevado de entidades que recopilan y utilizan datos, para que los individuos puedan gestionar toda la información que les proporcionan;
- un problema de agregación, que puede provocar usos derivados de los datos;
- un problema relativo a la complejidad para sopesar los daños provocados por la violación de la privacidad.

Este último lo presenta referido a tres cuestiones:

- muchos problemas de privacidad se producen a largo término o aparecen debido al uso derivado de los datos;
- los daños a la privacidad son a menudo pequeños y dispersos, pero unidos pueden ser perjudiciales y tener un impacto para los demás,
- el paradigma actual sólo da importancia a los daños ocasionados por usos no-consensuados de los datos (**Solove**, 2013).

Solove focaliza su análisis en la dificultad de los individuos para sopesar los costes y beneficios de la cesión de datos. Argumenta que es esta dificultad la que provoca que su decisión no sea significativa. Los problemas que Solove define como cognitivos, no son una cuestión diferente de aquellos estructurales, sino una consecuencia de ellos, que merman la capacidad de las personas para gestionar su privacidad.

En segundo lugar, una crítica a la falta de racionalidad humana no puede ser considerada una cuestión que afecte de forma especial al funcionamiento del modelo *notice and choice* en particular, sino una forma particular de comprender al ser humano.

Y por otra parte, toda ley presupone, en mayor o menor medida, una capacidad humana para decidir racionalmente, y no parece adecuado construir un paradigma legal basado en la capacidad racional de los individuos para sopesar los costes y los beneficios de unas acciones sobre las que no tienen control.

En el presente artículo se considera que las personas sí tienen una capacidad para decidir racionalmente, y que, en todo caso, el problema de protección de la privacidad no se debe a una falta de capacidades individuales, sino a una imposibilidad para actuar mediante los mecanismos disponibles.

El paternalismo libertario

Muchos, explica Solove, consideran que la solución a esta falta de capacidad de los individuos para decidir significativamente, de la que él habla, pasa por vías paternalistas, es decir, por la actuación ajena a la voluntad individual. Solove comprende que el paternalismo supone una interferencia directa en la voluntad del individuo y por lo tanto lo considera algo profundamente negativo. De aquí surge su "Dilema del consentimiento" (**Solove**, 2013, p. 1894). Su solución al dilema se recoge en lo que él llama el "paternalismo libertario": combinar la decisión individual con una serie de ayudas al afectado para decisiones complejas, y proporcionar un conjunto de normas básicas para cuestiones extremas, dirigida aquellos que utilicen los datos. Ambas vendrían determinadas de forma externa a la voluntad de los individuos. Además, propone que el modelo debería admitir la decisión selectiva en base a casos y el seguimiento continuado del uso de los datos, con la posible ayuda de una agencia gestora.

Tras analizar el *modelo mixto*, se extrae que la crítica a la falta de racionalidad de los individuos es, precisamente, lo que hace a Solove ver la necesidad de una solución paternalista. Si se entiende que la falta de capacidades de los individuos es una consecuencia de los problemas estructurales, el paternalismo no es necesario. Lo necesario es solventar dichos problemas. En este sentido parece anterior la necesidad de asegurar que los mecanismos de protección (la notificación y el consentimiento individual) sean adecuados en relación a aquello que se debe gestionar (los datos personales) y a cómo se debe gestionar (teniendo en cuenta la lógica *big data*). Si no es así, el individuo podría verse obligado a decidir bajo una falta de capacidades y de recursos, y en un sentido que no responda necesariamente a sus propias convicciones ni a sus intereses.

5.2. Una cuestión esencial

El mayor punto de divergencia del presente artículo con el *modelo mixto* es que en él no se abordan los problemas estructurales como la causa de la falta de capacidades de los individuos y que, al igual que en el modelo *notice and choice*, no se comprende que éstos suponen una barrera para la decisión libre.

Como resultado, se entiende que el modelo no sólo falla en la misma cuestión fundamental que el modelo *notice and choice* –comprender la libertad desde una perspectiva limitada-, sino que es todavía más inadecuado en su conceptualización de la privacidad (como un valor contextual relativo a daños) y en su propuesta de solución al problema (el "paternalismo libertario").

> La privacidad no debe ser un mero valor contextual, ni entrar en un juego de preferencias como moneda de cambio

6. Libertad para la privacidad

Hemos argumentado que el modelo *notice and choice* y el *modelo mixto* son insuficientes, y sus planteamientos inadecuados, para dar respuesta a la causa y al impacto de los problemas de privacidad derivados del fenómeno *big data*. Por ello parece necesario revisarlos. Desde el presente artículo se aduce que esto pasa por modificar el ideal de libertad individual que fundamenta el modelo de gestión de la privacidad de datos personales, al haber sido identificado como el principal problema de base en los dos modelos analizados. Entendemos que esto permitiría operativizar una concepción más amplia del valor de la privacidad como un valor integrador de la estructura social, que estaría en grado de generar mecanismos más adecuados.

6.1. Una concepción alternativa de libertad

El liberalismo, explica García-Manrique, ha defendido históricamente que "una cosa es ser libre de X y otra ser capaz de X" (**García-Manrique**, 2013, p. 155). Él, por el contrario, presenta la capacidad como una cuestión no separable de la libertad. Entiende la libertad como la capacidad del individuo para ejercer su autonomía, es decir, para elegir un plan de vida valioso y vivir de acuerdo con él (**García-Manrique**, 2013, p. 155). Esta idea de libertad responde a la concepción republicana y tiene como uno de sus máximos exponentes a Pettit, que concibe la libertad como no-dominación (**Pettit**, 1999, p. 77). La perspectiva republicana representa una alternativa al ideal liberal de la no-interferencia, que como se ha argumentado, recogen los modelos analizados en este artículo.

La concepción liberal entiende por interferencia únicamente un tipo de intervención directa en la voluntad del individuo para decidir su curso de acción (**Pettit**, 2004, p. 120).

La republicana reconoce tanto las interferencias directas como las indirectas y plantea que es imprescindible distinguir entre aquellas no-arbitrarias o legítimas y aquellas arbitrarias o ilegítimas (**Pettit**, 2004, p. 199). Determinar qué interferencias son legítimas es sin duda algo complejo, que presupone una cierta idea de lo que es una vida humana buena. No se profundizará en esta cuestión. Lo que aquí interesa destacar es, simplemente, que ésta atribución de legitimidad a las interferencias es justamente lo que hace a la concepción republicana más precisa que la liberal: mientras la visión liberal considera que las interferencias que van en contra de la libertad son aquellas que interfieren de forma directa en el curso de acción del individuo, la republicana entiende que las interferencias que van en contra de la libertad son aquellas arbitrarias, o no justificadas (sean directas o indirectas). Al contemplar estas interferencias indirectas la concepción republicana reconoce la posibilidad de que un sujeto merme la capacidad de otro para actuar, sin interferir de forma directa en sus acciones. Éste es otro punto diferencial de la concepción republicana que, mediante este reconocimiento, recoge la importancia del elemento de poder (y por consiguiente, de la desigualdad de poder) en la libertad. En este sentido, asume la necesidad de distribuir una serie de recursos fundamentales, que satisfagan ciertas necesidades básicas, y proporcionen a todos por igual la capacidad para ejercer la libertad.

7. Conclusiones

La manera de relacionarse y compartir información con los demás ha cambiado. Vivimos en un ecosistema de datos sociales masivos. La cantidad de información personal que existe se dispara, pero su generación y difusión no son algo exclusivamente personal, ni controlable por el individuo al que pertenece. Las técnicas y los métodos de recogida y procesamiento *big data* evolucionan con rapidez. Los objetivos del tratamiento de datos se centran en encontrar relaciones a gran escala, vislumbrar atributos y patrones latentes en los datos e inferir información que no ha sido proporcionada de forma explícita. Así, la analítica de datos masivos impide determinar de forma aislada y previa a dicho tratamiento qué datos deben ser considerados personales. Hoy, la privacidad de nuestros datos está interconectada. Su violación puede ser imprevisible y adquiere una dimensión colectiva. Preservar la privacidad en este escenario es complicado, es algo que trasciende las capacidades y los conocimientos de los individuos. Al mismo tiempo la complejidad y la opacidad intencionada de los sistemas de procesamiento de datos masivos aumentan la desigualdad de poder de los individuos frente a los grandes poderes corporativos y gubernamentales que se benefician de los datos.

> Los comportamientos de las personas con respecto a la difusión de su información personal no se corresponden con su preocupación por la privacidad

Paradójicamente, el paradigma de autogestión de la privacidad reinante en el mundo occidental carga al individuo el peso de proteger su privacidad, con la intención de asegurar que dicha gestión sea libre. Las limitaciones estructurales expuestas a lo largo de este artículo no representan una interferencia directa en la voluntad de los individuos, no les obligan a consentir o les prohíben desaprobar el uso de sus datos. Por ello, el ideal liberal que fundamenta el paradigma de la autogestión no las contempla como una barrera para la protección ni la libre gestión de la privacidad. El *modelo mixto* propuesto por Solove como alternativa al modelo *notice and choice* falla en esta misma cuestión fundamental.

El incremento de la cantidad de datos abre un gran abanico de oportunidades para el desarrollo social y es importante estudiar cuáles son y cómo se pueden explotar, pero ello requiere de una profunda reflexión sobre el valor de la privacidad en nuestros días y sobre la libertad de los individuos para preservarla. La privacidad es un derecho fundamental que debe garantizarse. Es un valor importante para el desarrollo justo y democrático de la sociedad y no sería beneficioso que se convierta en una moneda de cambio.

Sorprende que los ciudadanos continúen cediendo su información personal, aparentemente de forma despreocupada, pese a que su preocupación por la privacidad es creciente. Sin embargo, la falta de recursos y herramientas disponibles, la falta de transparencia, de control y de responsabilidad sobre de los procesos a los que se someten los datos y, en definitiva, la desigualdad de poder a la que se enfrentan los ciudadanos, podrían estar provocando que éstos se vean forzados a decidir en un sentido que no responda necesariamente a sus propias convicciones ni a sus intereses. Éstas son algunas de las cuestiones que necesitan respuesta si queremos acercarnos a una verdadera solución al problema.

> Es necesario asegurar la libertad de las personas para proteger su privacidad y, para ello, fomentar que todas tengan la capacidad y los recursos necesarios

Es necesario repensar los fundamentos conceptuales del paradigma actual, que están desvinculados de la lógica y los objetivos del procesamiento de datos masivos. Los mecanismos de protección de la privacidad deben abordar el impacto del uso de datos masivos, tanto en el nivel individual de la privacidad, como en el colectivo. Asimismo, los individuos deben tener libertad para proteger su privacidad y por ello se debe asegurar que todos tengan la capacidad de hacerlo. Pensar en los aspectos comunes que requieren el resguardo de la privacidad es posible y podría ser un buen punto de partida, entre otras cosas, para determinar qué capacidades se deben fomentar entre la ciudadanía, qué barreras se deben imponer, qué recursos se deben asegurar y qué mecanismos de actuación se deben proporcionar.

A fin de disipar posibles confusiones, lo que aquí se defiende no es el paso de una concepción individualista, que no reconoce el problema estructural que afecta a la protección de la privacidad, a su opuesto colectivista, donde el individuo y su decisión no tengan cabida. Este artículo es una defensa de la libertad para tomar decisiones valiosas para la propia vida, mediante los propios recursos y capacidades. Es una defensa de la libertad individual para proteger la privacidad de los datos personales (de todos) en la era de los *big data*.

8. Bibliografía

Agencia Española de Protección de Datos (2011). *El derecho fundamental a la protección de datos: Guía para el ciudadano.*
https://goo.gl/8IvsGx

Barnes, Susan B. (2006). "A privacy paradox: Social networking in the United States". *First Monday*, v. 11, n. 9, pp. 1-10.
https://goo.gl/PBn0vx

Baruh, Lemi; **Popescu, Mihaela** (2015). "Big data analytics and the limits of privacy self-management". *New media & society*, pp. 1-18.
https://doi.org/10.1177/1461444815614001

Berlin, Isaiah (1988). "Dos conceptos de libertad". En: Berlin, Isaiah. *Cuatro ensayos sobre la libertad*. Madrid: Alianza Editorial.
http://terras.edu.ar/biblioteca/10/10FP_Berlin_Unidad_3.pdf

Bertomeu, María-Julia; **Domènech, Antoni** (2005). "El republicanismo y la crisis del rawlsismo metodológico (Nota sobre método y sustancia normativa en el debate republicano)". *Isegoría*, n. 33, pp. 51-75.
https://goo.gl/yHd7JC

Bobbio, Norberto (2009). *Igualdad y libertad.* Barcelona: Ediciones Paidós Ibérica SA. ISBN: 978 8475098623

Bogomolov, Andrei; **Lepri, Bruno**; **Staiano, Jacopo**; **Oliver, Nuria**; **Pianesi, Fabio**; **Pentland, Alex** (2014). "Once upon a crime: Towards crime prediction from demographics and mobile data". En: *Procs of the 16th intl conf on multimodal interaction*.
https://arxiv.org/pdf/1409.2983.pdf

Boyd, Danah (2012). "Networked privacy". *Surveillance & society*, v. 10, n. 3/4, pp. 348-350.
http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/networked/networked

Boyd, Danah (2016). "Transparency ≠ Accountability". *Points: Experimental collection from data & society*, 29 Nov.
https://points.datasociety.net/transparency-accountability-3c04e4804504#.fsmuihtp6

Boyd, Danah; **Crawford, Kate** (2011). "Six provocations for big data". En: *A decade in internet time: Symposium on the dynamics of the internet and society*, Oxford Internet Institute.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431

Boyd, Danah; **Levy, Karen**; **Marwik, Alice** (2014). *The networked nature of algorithmic discrimination*. Open Technology Institute; New América; Data & Discrimination.
http://www.danah.org/papers/2014/DataDiscrimination.pdf

Burkell, Jacquelyn; **Fortier, Alexandre**; **Yeung-Cheryl-Wong, Lorraine**; **Simpson, Jennifer-Lynn** (2014). "Facebook: Public space, or private space?". *Information, communication & society*, v. 17, n. 8, pp. 974-985.
https://www.researchgate.net/publication/278401946_Facebook_Public_space_or_private_space
https://doi.org/10.1080/1369118X.2013.870591

Capella, Joseph N.; **Yang, Sijia**; **Lee, Sungkyoung** (2015). "Constructing recommendation systems for effective health messages using content, collaborative, and hybrid algorithms". *Annals of the American Academy of Political and Social Science*, v. 659, n. 1, pp. 290-306.
https://doi.org/10.1177/0002716215570573

Caplan, Robyn; **Boyd, Danah** (2016). "Who controls the

public sphere in an era of algorithms? Mediation, automation, power". *Data & society*, February 26.
https://datasociety.net/events/who-controls-public-sphere

Castillo, Carlos (2016). *Big crisis data*. Cambridge University Press. ISBN: 978 1107135765

Chen, C. L. Philip; **Zhang, Chun-Yang** (2014). "Data-intensive applications, challenges, techniques and technologies: A survey on big data". *Information sciences*, v. 275, pp. 314-347.
https://goo.gl/ilnlQu
https://doi.org/10.1016/j.ins.2014.01.015

Cox, Michael; **Ellsworth, David** (1997). *Application controlled demand paging for out-of-core visualization*. Report NAS-97-010, July 1997. Moffet Field: NASA Ames Research Centre.
https://www.nas.nasa.gov/assets/pdf/techreports/1997/nas-97-010.pdf

DeLorenzi, Daniel; **Shane, Jon M.**; **Amendola, Karen-L.** (2006). "The CompStat process: Managing performance on the pathway to leadership". *The police chief. The professional voice of law enforcement*, v. 73, n. 9.
http://www.nashville.gov/Portals/0/SiteContent/Finance/docs/OMB/Strategic%20Management/CompStat.pdf

Dockray, Sean (2010). The *Facebook* suicide bomb manifesto, *Wired*.
https://www.wired.com/2010/05/the-facebook-suicide-bomb-manifesto

Durán-Segura, Mercedes; **Mejías-Peligro, Juan-Francisco** (2014). "Conocimientos y comportamientos de los usuarios de la red social *Facebook* relacionados con la privacidad". Ámbitos. Revista internacional de comunicación. *Infoxicación*, n. 26.
http://institucional.us.es/ambitos/?p=1198

España (1999). "Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal". *BOE*, n. 298, 14 de diciembre.
https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Facebook for business (2014). "Learn more about the people that matter to your business with Facebook audience insights". *Facebook for business*, 8 May.
https://www.facebook.com/business/news/audience-insights

Fernández-Manzano, Eva-Patricia; **Neira, Elena**; **Clares-Gavilán, Judith** (2016). "Data management in audiovisual business: *Netflix* as a case study". *El profesional de la información*, v. 25, n. 4, pp. 568-576.
https://doi.org/10.3145/epi.2016.jul.06

García-Manrique, Ricardo (2013). *La libertad de todos. Una defensa de los derechos sociales*. Barcelona: El viejo topo. ISBN: 978 8415216513

Gouveia-Rodrigues, Ramón; **Marques-das-Dores, Rafael**; **Camilo-Junior, Celso G.**; **Couto-Rosa, Thierson** (2014). "SentiHealth-cancer: A sentiment analysis tool to help detecting mood of patients in online social networks". *International journal of medical informatics*, v. 85, n. 1, pp. 80-95.
https://doi.org/10.1016/j.ijmedinf.2015.09.007

Halavais, Alexander (2015). "Bigger sociological imaginations: Framing big social data theory and methods". *Information, communication & society*, v. 18, n. 5, pp. 583-594,
https://doi.org/10.1080/1369118X.2015.1008543

Hallinan, Blake; **Striphas, Ted** (2016). "Recommended for you: The Netflix Prize and the production of algorithmic culture". *New media & society*, v. 18, n. 1, pp. 117-137.
https://doi.org/10.1177/1461444814538646

Hargittai, Eszter; **Marwik, Alice** (2016). "What can I really do?" Explaining the privacy paradox with online apathy". *International journal of communication*, v. 10, pp. 3737-3757.
http://ijoc.org/index.php/ijoc/article/view/4655

He, Wu; **Shen, Jiancheng**; **Tian, Xin**; **Li, Yaohang**; **Akula, Vasudeva**; **Yan, Gongjun**; **Tao, Ran** (2015). "Gaining competitive intelligence from social media data. Evidence from two largest retail chains in the world". *Industrial management & data systems*, v. 115, n. 9, pp. 1622-1636.
https://doi.org/10.1108/IMDS0320150098

Hobbes, Thomas (2011). *Leviatán o la materia, forma y poder de un estado eclesiástico y civil*. Madrid: Alianza Editorial. ISBN: 978 8420682808

Hoy, Mariea-Grubbs; **Milne, George** (2013). "Gender differences in privacy-related measures for young adult Facebook users". *Journal of interactive advertising*, v. 10, n. 2, pp. 28-45.
https://goo.gl/OHn7Gl
https://doi.org/10.1080/15252019.2010.10722168

Jourová, Vêra (2016). "How will the EU's reform adapt data protection rules to new technological developments?". *European Commission, Justice and Costumers*.
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404

Karppi, Tero (2011). "Digital suicide and the biopolitics of leaving *Facebook*". *Transformations. Journal of media and culture*, n. 20, pp. 1-18.
http://www.transformationsjournal.org/issues/20/article_02.shtml

Karppi, Tero; **Crawford, Kate** (2016). "Social media, financial algorithms and the hack crash". *Theory, culture & society*, v. 33, n. 1, pp. 73-92.
https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2602857
https://doi.org/10.1177/0263276415583139

Kroll, Joshua A.; **Huey, Joanna**; **Barocas, Solon**; **Felten, Edward W.**; **Reidenberg, Joel R.**; **Robinson, David G.**; **Yu, Harlan** (2016). "Accountable algorithms". *University of Pennsylvania law review*, v. 165.
https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2765268

Laney, Doug (2001). "3D data management: Controlling data, volume, velocity and variety". *Application delivery strategies*. Meta Group Inc., Stamford.
https://goo.gl/CBdMXf

Manovich, Lev (2012). "Trending: the promises and the challenges of big social data". En: Gold, Matthew K. *Debates in the digital humanities*. Arizona: University of Minnesota

Press, pp. 460-475.
http://dhdebates.gc.cuny.edu/debates/text/15

Martin, Kirsten (2015). "Understanding privacy online: Development of a social contract approach to privacy". *Journal of business ethics*, v. 137, n. 3, pp. 551-569.
https://doi.org/10.1007%2Fs10551-015-2565-9

Mayer-Schönberger, Victor; **Cukier, Kenneth** (2013). *Big data. A revolution that will transform how we live, work and think*. Londres: John Murray. ISBN: 978 1848547926

Metcalf, Jacob; **Crawford, Kate** (2016). "Where are human subjects in big data research? The emerging ethics divide". *Big data and society*.
https://doi.org/10.1177/2053951716650211

Minelli, Michael; **Chambers, Michele**; **Dhiraj, Ambiga** (2013). *Big data, big analytics*: *Emerging business intelligence and analytic trends for today's businesses.* John Wiley & Sons. ISBN: 978 1118562260
https://doi.org/10.1002/9781118562260

Pasquale, Frank (2015). *The black box society. The secret algorithms that control money and information*. London: Harvard University Press. ISBN: 978 0674368279

Pettit, Philip (1999). *Republicanismo. Una teoría sobre la libertad y el gobierno*. Barcelona: Paidós. ISBN: 978 8449306891

Pettit, Philip (2004). "Liberalismo y republicanismo". En: Ovejero, Félix; Gargarella, Roberto; Martí, José-Luis (eds.). *Nuevas ideas republicanas: autogobierno y libertad*. Barcelona, Paidós, pp. 115-135. ISBN: 978 8449315107

Pohl, Daniela; **Bouchachia, Abdelhamid**; **Hellwagner, Hermann** (2015). "Social media for crisis management: Clustering approaches for sub-event detection". *Multimedia tools and applications*, v. 74, n. 11, pp. 3901-3932.
https://goo.gl/efb7FU
https://doi.org/10.1007/s11042-013-1804-2

Popescu, Mihaela; **Baruh, Lemi** (2013) "Captive but mobile: Privacy concerns and remedies for the mobile environment". *The information society*, v. 29, n. 5, pp. 272-286.
https://doi.org/10.1080/01972243.2013.825358

Privacy-International (s.f.). *Metadata*.
https://privacyinternational.org/node/573

Richardson, Janice (2016). *Law and the philosophy of privacy*. Londres: Routledge. ISBN: 978 0415572439

Sarker, Abeed; **Ginn, Rachel**; **Nikfarjam, Azadeh**; **O'Connor, Karen**; **Smith, Karen**; **Jayaram, Swetha**; **Upadhaya, Tejaswi**; **Gonzalez, Graciela** (2015). "Utilizing social media data for pharmacovigilance: A review". *Journal of biomedical informatics*, v. 54, pp. 202-212.
https://doi.org/10.1016/j.jbi.2015.02.004

Schroeck, Michael; **Shockley, Rebeca**; **Smart, Janet**; **Romero-Morales, Dolores**; **Tufano, Peter** (2012). *Analytics: The real-world use of big data. How innovative enterprises extract value from uncertain data*. IBM Institute for Business Value.
https://goo.gl/vUCcwL

Schwartz, Paul M. (2013). "The EU-US privacy collision: A turn to institutions and procedures". *Harvard law review*, v. 126, n. 7, pp. 1966-2009.
http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_schwartz.pdf

Solove, Daniel J. (2008). *Understanding privacy*. Cambridge: Harvard University Press. ISBN: 978 067402772

Solove, Daniel J. (2013). "Introduction: Privacy self-management and the consent dilemma". *Harvard law review*, v. 126, n. 7, pp. 1880-1903.
http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Taddicken, Monika (2014). "The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure". *Journal of computer-mediated communication*, v. 19, n. 2, pp. 248-273.
https://doi.org/10.1111/jcc4.12052

Tufekci, Zeynep (2014). "Big questions for social media big data: Representativeness, validity and other methodological pitfalls". En: *Procs of the 8th Intl AAAI Conf on weblogs and social media*.
https://arxiv.org/abs/1403.7400

Turow, Joseph; **Hennessy, Michael**; **Draper, Nora** (2015) *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Annenberg School for Communication University of Pennsylvania.
https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Unión Europea (1995). "Directiva 95/46/CE del Parlamento Europeo y del Consejo, 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos". *Diario oficial de la Unión Europea*, n. L 282 de 23 de noviembre, pp. 0031-0050.
http://www.wipo.int/wipolex/es/details.jsp?id=13580

Unión Europea (2016). "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)". *Diario oficial de la Unión Europea*, n. L119 de 4 de mayo.
https://goo.gl/cAVmfJ

Utz, Sonja; **Kramer, Nicole C.** (2009). "The privacy paradox on social network sites revisited: The role of individual characteristics and group norms". *Cyberpsychology: Journal of psychosocial research on cyberspace*, v. 3, n. 2, pp. 1-10.
http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1

Xiao, Yu; **Huang, Qunying**; **Wu, Kai** (2015). "Understanding social media data for disaster management". *Natural hazards*, v. 79, n. 3, pp. 1663-1679.
https://doi.org/10.1007/s11069-015-1918-0

4

Suárez-Gonzalo, Sara (2018). Your likes, your vote? Big personal data exploitation and media manipulation in the US presidential election campaign of Donald Trump in 2016, *Quaderns del CAC, XXI*(44): 25-33.

Disponible en: https://www.cac.cat/sites/default/files/2019-01/Q44_Suarez_EN_1.pdf.

ISSN electrónico: 2014-2242.

ISSN (online): 2014-2242 / www.cac.cat

QUADERNS
DEL CAC

Your likes, your vote? Big personal data exploitation and media manipulation in the US presidential election campaign of Donald Trump in 2016

Sara Suárez-Gonzalo
Predoctoral researcher in the Department of Communication at Pompeu Fabra University

sarapaz.suarez@upf.edu
ORCID Code: orcid.org/0000-0001-6883-1984.

Article received on 23/04/2018 and accepted on 11/07/2018

Abstract

The newspapers Observer *and* The New York Times *have revealed an alleged massive-scale scandal of data corruption involving Facebook and Cambridge Analytica that could have benefited the electoral victory of Donald Trump.*

The objective of this article is to analyze the conditions of possibility of the case and its potential influence on Americans' voting decision. To do so, it examines the scientific-technological, business and legal context related to big data technologies in which the facts would have happened and evaluates their possible influence in relation to the limits of the performed strategy and its current media and socio-political context.

Keywords

Big data, personal data protection, Donald Trump, Facebook, Cambridge Analytica, media manipulation.

Resum

Els diaris Observer *i* The New York Times *han revelat un suposat escàndol de corrupció de dades a escala massiva que involucra Facebook i Cambridge Analytica i que podria haver afavorit la victòria electoral de Donald Trump.*

L'objectiu d'aquest article és analitzar les condicions de possibilitat del cas i de la seva influència potencial en la decisió de vot nord-americà. Per a això s'examina el context cientificotecnològic, empresarial i legal relacionat amb les tecnologies big data en el qual s'haurien produït els fets, i es valora la seva possible influència en relació amb les limitacions pròpies de l'estratègia emprada i el seu context mediàtic i sociopolític actual.

Paraules clau

Big data*, protecció de dades personals, Donald Trump, Facebook, Cambridge Analytica, manipulació informativa.*

Introduction

On March 17, 2018, the newspapers *Observer* and *The New York Times* published the testimony of a new "whistleblower" named Christopher Wylie. The news reports revealed the supposed improper transfer of the data of millions of Facebook users to the company Cambridge Analytica, along with the fact that this company may have used these data to favour the victory of Donald Trump in the 2016 US general elections via a micro-targeting strategy based on military psychological attack techniques. It also reported that some of the data collected in the United Kingdom may have been used in the "Vote Leave" and "BeLeave" campaigns to push for the vote in favour of Brexit in the referendum held on the 23rd of June 2016.

Due in part to media leaks like this one, which is related to data corruption and the possibilities currently afforded by big data gathering and analytics technologies, citizen concern over the privacy of personal data has increased in recent years (Hargittai & Marwick 2016; Turow, Hennessy & Draper 2015). Despite the fact that big data analytics are still a more developed form of quantitative analysis, there are major new developments: data collection is indiscriminate and their processing draws from aggregation and cross-referencing techniques (Baruh & Popescu 2015) which enable information to be inferred from data even if it is not explicitly contained therein (Tufekci 2015). Different academic disciplines have made a decisive contribution to the technical development of the possibilities afforded by big data analytics and to reduce its costs. As a result, organisations and public and private institutions have already begun to use big data for different purposes. Market predictions, targeted advertising, improvements in the transport sector, the pursuit of terrorists, public health and the management of natural disasters are just several examples (European Parliament Resolution, 14 March 2017). However, beyond this, a business model has begun to gain ground that is based on data exploitation and dominated by large tech multinationals.

Big data technologies are not only increasingly complex, but they are also particularly opaque (Pasquale 2015), given that

there are major power interests at stake in data exploitation. For this reason, the 'notice and choice' model (Baruh & Popescu 2015) underlying Western data-protection laws is insufficient to deal with the social impact of big data phenomenon (Suárez-Gonzalo 2017).

Just like any technological advance, big data gathering and analysis methods and tools run the risk of falling into the wrong hands or being misused. The Cambridge Analytica case exemplifies this danger, but beyond that it also illustrates many of the risks entailed in the current development of big data. On the one hand, it reveals the threats that it poses to privacy and personal data protection, as well as the inadequacies of the current laws. On the other hand, it allows us to debate its influence on the rise in media manipulation, online disinformation and the radicalisation of ideas and political opinions (Marwick & Lewis 2017).

The aim of this article is to show that the seriousness of the Cambridge Analytica case is more closely associated with the existence of a structure that makes it possible and its social impact, as opposed to the possible specific interference it exercised on voting decisions in the United States. To fulfil this objective, the article is divided into two parts. In the first part, it offers a description of the facts reported by *Observer* and *The New York Times* and analyses the conditions that made this possible in relation to the characteristics of the scientific-technological, business and legal context in which it happened. It is important to stress that this article focuses on the US side of the case, which was the one that garnered the most attention and where more information has been confirmed so far through other sources. On the other hand, given that the publication of the information is still very recent and that these are not proven facts, it should be stressed that the argumentation presented in this study does not depend on the veracity or accuracy of the deeds but on an analysis of the conditions that made them possible. Through this analysis, I am seeking to explain that far from being the cause of the problem, this case is its expected consequence. The second part focuses on the possible influence of the Cambridge Analytica case. Following the same logic as in the first part, in the second I explain the kind of influence that the technique of micro-targeting exerts on people. Then, the level of this influence on the US vote is questioned in relation to the limitations of the model used to develop the profile of the target audience of that campaign on the one hand, and according to the current media and sociopolitical context within which the case falls on the other.

In order to fulfil this objective, three main sources are used: scholarly, journalistic and corporate. Given the theoretical nature of the study, the scholarly output is the most relevant source and serves as the foundation of the argumentation developed. Secondly, journalistic sources are used to explain the Cambridge Analytica case. After consulting a large corpus of news reports, the two published by the *Observer* and one published by *The New York Times* (the media outlets which had the scoop on the case) on the 17th of March 2018 (the day when the case was revealed) were chosen, as they contain more detailed information on the deeds. These three are joined by a fourth source published by *Observer* one year before the leak (7 May 2017), when the newspaper began to reveal relevant information from the confession of an informant who was still shrouded in anonymity. Finally, two kinds of corporate sources were examined: first, the websites of the companies involved (Cambridge Analytica and SCL Group), where they describe their own business model, and secondly notifications and official reports on the case published on Facebook.

Your digital life, Cambridge Analytica and the Trump election campaign

The last Facebook estimation (Schroepfer, 4 April 2018) confirms that in 2014 the data of approximately 87 million Facebook users were leaked to the company Cambridge Analytica. Of this 87 million, more than 70 were profiles of US citizens. More than one million of the remainder were citizens of the United Kingdom, and almost 137,000 were Spaniards.

Data collection

According to the testimony of a former Cambridge Analytica and SCL Group employee, Christopher Wiley, published by *Observer - The Guardian* (Cadwalladr & Graham-Harrison, 17 March 2018; Cadwalladr, 17 March 2018) and by *The New York Times* (Rosenberg, Confessore & Cadwalladr, 17 March 2018), the transfer of these data would have taken place thanks to the involvement of Cambridge University professor and researcher Aleksandr Kogan. He would have replicated the *myPersonality* application developed by his colleagues in the Psychology department, whose results were disseminated in a scholarly publication in 2012 (Stillwell & Kosinski 2012). The replica seems to have been *This is Your Digital Life*, a personality test available on Facebook since 2014, which required its participants to have a Facebook account and be US voters. When participating, the users consented to allow the data in their account to be used for academic research, and in exchange they received monetary compensation. According to the data that Zuckerberg made public (21 March 2018), almost 300,000 people performed the test. However, *This is Your Digital Life* also gave Kogan access to certain information on the "friends" of the majority of participants in the test, in such a way that the number of user profiles whose data he obtained increased exponentially to 87 million. Because these "friends" had not consented to his accessing their profiles, the data obtained from them were fundamentally those generated by their participation in the social media, which are usually "public by default".

According to Wiley (Cadwalladr & Graham-Harrison, 17 March 2018), Kogan would have leaked these data to Cambridge Analytica in 2015 via a commercial agreement between his company Global Science Research (GSR) and SCL Elections, a

subsidiary of SCL Group, which is, in turn, a company affiliated with Cambridge Analytica. This leak was not discovered by Facebook until approximately one year later, in 2015, and it then failed to inform either its affected users or the States about the leak.

The recent reports and official publications shared by the Facebook authorities (Grewal, 16 March 2018; Schroepfer, 4 April 2018; Zuckerberg, 21 March 2018) confirm Wiley's testimony. Now, the Facebook Help Centre has made available to users the tool called "How to check if your Facebook data was used by Cambridge Analytica" (Facebook 2018), where they can check whether the data company had accessed the information in their profile.

Data analysis

Wiley would have used the method developed by Stillwell and Kosinski (2012), Kosinski, Stillwell and Graepel (2013) and Youyou, Kosinski and Stillwell (2015) to conduct psychometric studies based on the data obtained from *myPersonality* (Stillwell & Kosinski 2012) to analyse the data collected via *This is Your Digital Life*. Kosinski, Stillwell and Graepel (2013) demonstrated the possibility of ascertaining highly sensitive personal attributes and characteristics by automatically analysing easily-accessible digital records of human behaviour, in this case "likes" on Facebook. The attributes the study demonstrated it could predict include sexual, political and religious orientation, sex, ethnicity and information on users' lives such as drug consumption, level of life satisfaction and whether or not a person's parents remained together until the individual was 21 years old. From this, Wiley would have gotten a description of the psychological profiles of millions of users involved, including their political affinities. The results of the personality test performed by the almost 300,000 people who participated in *This is Your Digital Life* would have been the control group to test the validity of the analyses performed on the entire data set.

According to the information published by The Guardian (Cadwalladr, 7 May 2017), Cambridge Analytica would have combined this psychological information extracted from databases of consumers and then crossed it with postal addresses, emails and telephone numbers. Until that time, Facebook itself allowed profile searches based on telephone numbers or addresses, an option which, as Schroepfer explained (4 April 2018), the company has now deactivated due to the abuses perpetrated by ill-intentioned users.

Data exploitation

The former Cambridge Analytica employee revealed that these data would have been used in a political micro-targeting campaign with the goal of influencing voting decisions during the 2016 presidential elections in favour of Donald Trump (Cadwalladr, 17 March 2018).

Newman (2016) claims that the micro-targeting technique was used in the Obama campaign committees in the 2008 and 2012 presidential elections. Micro-targeting is a direct advertising technique which allows more persuasive campaigns to be generated by using big data analytics techniques and artificial intelligence mechanisms to get information and target the audience in a more personalised fashion (Alkış & Taşkaya Temizel 2015; Miralles-Pechuán, Ponce & Martínez-Villaseñor 2017; Neumann 2017).

However, in the Trump campaign, Christopher Wiley (Cadwalladr, 17 March 2018) points to the use of psychological operations (PSYOPS), a kind of military information warfare technique that seeks to exert a manipulative, not persuasive, influence. PSYOPS are a type of attack which consists in locating targets that are particularly vulnerable to psychological impact and launching a message that is capable of changing their feelings in order to urge them towards a particular action that favours national or allied interests. The US defence forces have waged this kind of information attack before, during or after wars and conflicts (United States Air Force 1999). The research undertaken by Briant (2018) argues that after the terrorist attack waged by Al Qaeda on the 11th of September 2001, the US government decided to extend the use of psychological operations to modern propaganda systems inside the country. In her article, Briant argues that this transformation is due largely to the spread of information and communication technologies which challenge the influence of the propaganda model traditionally used by the US Bureau of Public Affairs. Sartonen, Simola, Timonen and Lovén (2017), in turn, underscore that one of the major potentialities of the psychological profiles yielded from the analysis of online behaviour is their ability to contribute to the objectives of *PSYOPS*.

The case, possible and necessary

First of all, in order to keep in mind the facts we are discussing, it should be noted that if Wiley's testimony is confirmed:

1. There would have been a massive data leak of Facebook users by means of a commercial agreement between the Cambridge University scholar Aleksandr Kogan and SCL Group.
2. In total, this leak would have affected the profiles of approximately 87 million Facebook users.
3. As a consequence, Facebook would have failed to fulfil its rule which requires anyone who gathers user data to inform users of the purpose and not to allow the data to be transferred to third parties. In the case of the affected European countries, Facebook would also have failed to comply with the European Data Protection Regulation (EU 2016/679), which bans the sale of data to third parties.
4. Furthermore, the agreement reached with users who participated in *This is Your Digital Life* would have been violated, as they only consented to provide access to their profile information for academic uses.
5. Subsequently, these data would have been used to

manipulate the voting decision of the US electorate in favour of the candidacy of Donald Trump through a micro-targeting campaign based on military information warfare techniques.

Despite the existence of reports that would, at least, partially confirm Wiley's testimony, the argumentation developed in this study does not depend on the veracity or accuracy of the data but on the existence of the scholarly research that that makes these deeds possible, a business model that needs them and a legal context that is incapable of dealing with it.

Thus, this section explains the main characteristics of the scholarly research, the business model and the legal context related to the case.

Data exploitation as an academic research line

Firstly, the scholarly publications mentioned in the previous section, which are essentially associated with the fields of Psychology, Computational Science and Communication, demonstrate:

1. That the automatic analysis of easily-accessible digital records on the behaviours of people in their social networks reveals a range of sensitive characteristics about their personality, including their political affinity (Kosinski, Stillwell & Graepel 2013; Stillwell & Kosinski 2012; Youyou, Kosinski & Stillwell 2015).
2. That based on the psychological profile obtained in the previous analysis, it is possible to develop more persuasive personalised communication strategies (Alkış & Taşkaya Temizel 2015; Miralles-Pechuán, Ponce & Martínez-Villaseñor 2017; Neumann 2017).
3. That people's psychological profile is of great interest in the application of military emotional manipulation techniques which are capable of modifying people's behaviours based on specific objectives (Sartonen, Simola, Timonen & Lovén 2017).

Due to the social risk entailed in this line of research, it seems essential to clearly stipulate which are its aims for social development and which are the fields in which its practical execution is legitimate.

Data exploitation as a business model

On the other hand, the companies involved in this case, Cambridge Analytica and SCL Group, embody an expanding business model which has the backing of multi-million-dollar investments. This consists in developing strategic communication campaigns whose objective is to modify the behaviour of vulnerable population segments from a given target audience in favour of specific objectives.

Cambridge Analytica (2018) is a company headquartered in New York, Washington and London which was founded in 2013 as a subsidiary of SCL Group. The CEO of the company in the United States, whose biggest investor is the US billionaire Robert Mercer, is Steve Bannon, former Senior White House Counsellor to Donald Trump. Under the slogan "Data drives all we do", Cambridge Analytica presents itself as a company that "uses data to change the audience's behaviour". The company is made up of a sales division devoted to advertising and marketing, and a political division devoted to electoral communication campaigns. The services it offers, whether targeted to consumers or voters, are: researching the target audience in order to learn about it in-depth and understand its main characteristics; adding and integrating the data obtained into a centralised platform; predicting audience segments likely to respond favourably to the messages; developing customised multi-channel campaigns to capture key audience segments; and reporting on their future scope through campaign performance data. It promises companies that they can learn about every individual in their target audience in order to help them connect with them "on a personal level". It promises its clients in the political division to identify their target electorate, learn more about them and gain more influence over them in order to spur them to action at a low cost. In other words, its business model consists in data exploitation to modify the target audience's behaviour.

In turn, SCL Group (2018) also belongs to Robert Mercer, and as stated on its website. It is a company devoted to developing strategic communication campaigns for governments and military organisations all over the world based on data analytics. Its main objective is to spark changes in behaviour in defence, intelligence and social-change operations.

With regard to the business model, therefore, it is essential to ensure that all the companies' private interests respect citizens' rights and the democratic organisation of society.

Legal insufficiency

Finally, if Wiley's testimony is confirmed, there would have taken place alleged illegalities related to data collection. This section shows that, beyond punishing these illegalities, the legal framework of personal data protection is insufficient to deal with the situation. The reflections are common to American and European cases, which are grounded upon the same individual 'notice and choice' model (Baruh & Popescu 2015). This requires people to be clearly informed about what happens to their data, since based on this information, they can provide their consent (or not) to give up the data.

Data accessibility

Given that the bulk of the information that Cambridge Analytica supposedly used to generate a strategy to influence the electorate is easily accessible (likes), the fact that it obtained them illegally does not seem overly relevant.

In this regard, it seems essential to point out the fact that just because the data are accessible does not mean that they are public. Social media interfaces are spaces designed and managed by private companies with certain commercial interests, and therefore they are not exactly comparable to

traditional public spaces. Besides, the fact that something is public does not mean that it can be used by anyone or for any purpose.

Invalid agreement

Likewise, by lying about the purpose of the data (commercial, not scholarly), there would have been a rupture in the agreement between the two parties: the research who asks for the user's consent to collect their data, and the user who provides it. Beyond this rupture in the agreement, which was punished by the social media itself, the Cambridge Analytica case shows that, as argued in a previous study (Suárez-Gonzalo 2017), individual consent is an invalid instrument to protect personal data, at least for these reasons:

1. It is a requirement to participate in and enjoy products and services. In the case of *This is Your Digital Life*, users had to accept the user conditions of both the Internet browser and those of Facebook and the application itself. Furthermore, in this case the cession of data seems to have been associated with monetary compensation.
2. Due to the capacity of big data analytics technologies to infer latent information in data, users consent to provide access to certain data in their profile but remain unaware of what sensitive information can be gotten by analysing these data (Tufekci 2015). This means that even though the footprints of our basic behaviour as social media users are not necessarily considered personal data, the information that can be extracted from analysing them can become extremely sensitive.
3. On the other hand, the personal information that a person disseminates also affects others, so a person is not necessarily aware of (or has not necessarily consented to) the publication of information that affects them. In this sense, individual consent has a social impact. The case of *This is Your Digital Life* exemplifies this issue in two ways. First, the fact that a group of people participated in the test has been used to harm millions of other people who have nothing to do with it. Secondly, the fact that these people gave their consent helps to shape a business model based on the exploitation of personal information that affects society as a whole.
4. This complexity is compounded by the intentional opacity of big data technologies (Pasquale 2015), which makes it particularly complex for people to be properly informed about what will happen to their data when they consent. This also means that the agreement reached via consent does not entail negotiation, nor does it take place between equal parties.

For these reasons, it is difficult to consider individual consent a valid method to protect personal data.

The influence, in its context

The section above focused on the characteristics of the context in which the Cambridge Analytica case occurred. This section focuses on the context related to the type and level of influence of the case.

Given the seriousness of the facts revealed, there is no doubt that a rigorous study of the veracity of the deeds and their level of influence on Donald Trump's victory is needed. However, focusing our attention exclusively on this matter may be futile, firstly because it is difficult to measure the level of influence that an isolated act has within a complex decision. Secondly, because this could lead us to minimise the importance of the fact that there is a business precisely model devoted to gaining this influence, and furthermore, because if big data technology continues developing in the same way as today, its capacity for influence will continue to grow.

The purpose of this section is to explain the importance of focusing on the social impact of the system which makes possible the Cambridge Analytica case, instead of the specific interference of the case in US voting decision. To do so, this section describes the kind of influence that micro-targeting technique exerts over people. It then questions this influence, on the one hand, in relation to the limitations of the model used to devise the profile of the target audience of that particular campaign and, on the other, in accordance with the current media and sociopolitical context of the case.

Persuasion or manipulation

According to Bennett (2015), the technique of micro-targeting incorporates the trends that are characteristic of current electoral campaign management in Western societies, such as: it uses big data technologies to collect and integrate the data on voters into unified management platforms, including their consumption data and the data generated on the social media, and it signals the shift from mass messages to targeting micro-audiences. Bennett claims that these techniques emerged as the outcome of the decreasing efficacy of traditional techniques. They are cheaper yet more intrusive ways of influencing voters' behaviours. He also notes that these trends are generating a consumerisation of the vote, and therefore they not only affect the individual's privacy but also broader democratic dynamics.

By defining an individualised audience profile, the technique of micro-targeting exposes the individual to certain information selectively. In this way, it does not explicitly say what to consume or whom to vote for but instead shapes some of the referents based on which people spend money and vote. Likewise, the fact that the individual is unaware which of their profiles the person targeting them is using when exposing them to this information places them in a position of being vulnerable to manipulation.

Yet another issue is the fact that Wiley's testimony cites the use of military techniques with a psychological impact. Even though this has not been proven, there are two factors that lead us to

mistrust it. On the one hand, the notable similarity between the range of services purveyed by the company Cambridge Analytica (2018) and the characteristics of the information attacks perpetrated by the US defence forces (United States Force 1999). On the other hand, the experience of SCL Group (2018) in developing strategic defence campaigns and its association with the military elites. This is joined by scholarly studies that show the potentiality of psychological profiles to undertake "psychological operations".

Biased profile

Micro-targeting is based on defining a precise, individualised profile of the target audience. In the case of the Trump campaign, this profile was devised based on the model developed by Cambridge University (Kosinski, Stillwell & Graepel 2013; Stillwell & Kosinski 2012; Youyou, Kosinski & Stillwell 2015). In this sense, when discussing the influence of the Cambridge Analytica case, it is essential to weigh the possible limitations of this model.

Big data technologies provide an overview of what is being studied, that is, a broad picture of the situation. What is not as clear is that through this picture is it possible to understand or explain complex phenomena such as psychology and human behaviour, which are not mathematical (Boyd & Crawford 2012). For this reason, it seems essential with a touch of scepticism the assumption that through the analysis of a given representation of human behaviour (likes), precise information can be gained on complex personality features (ideology). In this sense, the application of big data analytics to human behaviour as in the case of *This is Your Digital Life* may mean that the profiles developed are biased. In this way, the potential influence exerted by the Trump campaign would be diminished.

Media context

The aim here is to relate the possible influence of the Cambridge Analytica strategy on the US decision to vote for Trump or Clinton with the current media context in which the US election campaign took place.

In a representative democratic system, freedom to elect political representatives is crucial. This requires, among other things, that citizens have access to truthful, diverse and plural information. For this reason, the traditional media, as well as the new social media, should be democratising tools serving the right to freedom of expression. However, media manipulation and disinformation are on the rise, and as a result the credibility of the media is being called into question (Marwick & Lewis 2017; HLEG 2018).

Marwick and Lewis (2017) argue that disinformation online and ideological radicalisation are consequences of online media manipulation. As the result of a deterioration in trust in the traditional media, the main actors in media manipulation (trolls, gamergaters, conspiracy theoreticians, influencers, haters, hyper-partisan news media and politicians) have found their space in blogs and websites, forums and message boards on the Internet and in the leading social media (such as Facebook, YouTube and Twitter). According to the authors, they are generally motivated by reasons related to ideology, money or the quest for status or acceptance. Thus, the circulation of memes and hoaxes, conspiracies against candidates, the use of bots and the distribution of fake news also played a major role in the election campaign for the US presidency (Marwick & Lewis, 2017). One example of this was the disinformation campaign promoted online about the Democratic candidate's purported ill health, which went viral and made the leap to the traditional media.

On the other hand, the developments in big data technology and artificial intelligence have led what is called the "algorithm culture" (Hallinan & Striphas 2016) to also affect information classification and hierarchisation. In recent years, the use of search engines on the Internet and the social media to check information has become very common (Nikolov, Oliveira, Flammini & Menczer 2015). During the peak of the US presidential elections, 62% of citizens got their information through the social media (Shearer & Gottfried 2017). Due to the multiplication of devices from which information is accessible, personalised recommendation systems have been developed as the best way to get news contents to Internet users in line with their interests (Yingyuan, Pengqiang, Hsu, Hongya & Xu 2015). Numerous recent studies (Borgesius, Trilling, Möller, Bodó, de Vreese & Helberger 2016; Dutton, Reisdorf, Dubois & Blank 2017; Holone 2016; Nicolov, Oliveira, Flammini & Menczer 2015) have focused on the impact of algorithm culture on the rise of disinformation and media manipulation. The majority concur that citizens are exposed to biased information which confirms and reinforces the thoughts and attitudes that they and people with views like theirs already have. This is known as the bubble effect or echo chambers.

On the other hand, the traditional media still play an important role in electoral campaigns. According to Marwick and Lewis (2017), the framing and strategic amplification of certain ideas or messages is one of the most common media manipulation techniques. Patterson (2016) states that the tone used in the media coverage was overwhelmingly negative, while the discussion of political issues was extremely light. However, he also concludes that the candidate Hillary Clinton was treated more negatively than her political rival. Foster, Shoaf and Parsons (2016) claim that gender stereotypes continue to harm female candidates in the media coverage of electoral campaigns. Likewise, the construction of the political frameworks (Oates & Moe 2016) or the different ways the candidates used the social media (Enli 2017) also played a major role in the electoral campaign.

This media context reveals at least three interesting issues which can help us assess the possible influence of the Cambridge Analytica case. First, it shows that the micro-targeting campaign waged by Cambridge Analytica is framed within the new forms of media manipulation related to the bubble effect. Secondly, this would not be the only influence

strategy to which citizens were exposed during the campaign. And finally, the interests of Trump and Cambridge Analytica were not isolated from the interests of the other actors and media influencing the campaign.

Social and political context

The explanations suggested for Trump's victory include many others that are not solely related to the media's actions. According to Gaughan (2016), some of them are related to the economic concerns of white working-class voters (which the Trump campaign managed to identify); the rise of racism and misogyny; the segregation and polarisation of the electorate (which, as seen in the previous section, could be related to media manipulation); the increase in income inequality; and the controversial actions of the FBI director. Thus, another important issue when discussing the influence of the Cambridge Analytica case is the political and social context in which the electoral campaign occurred. Fraser (2017) claims that Trump's win is part of a series of political events that have recently occurred worldwide. They include the triumph of Brexit, Bernie Sanders' campaign in the Democratic Party primaries in the US, the rejection of Matteo Renzi's reforms in Italy and the increased support of Marine Le Pen's National Front in France. These events, explains Fraser, represent citizen pushback to the effects of globalisation, as well as to a new form of "progressive neoliberalism" and the ruling classes that have promoted it. Trump, Fraser says, captured part of the electorate thanks to a "reactionary populism" which was opposed to the mixture of truncated ideals of emancipation and lethal forms of financialisation represented by "progressive neoliberalism".

Conclusions

The argumentation throughout this article gives rise to at least the following conclusions:

1. The Cambridge Analytica case is the probable consequence of a given scientific-technological structure, a business model and a legal framework that make it possible and necessary.
2. Focusing attention on the level of influence that the Cambridge Analytica strategy may have had in the US voting decision is not useful in helping us understand the seriousness of the situation for these four reasons: it deflects attention from the structures sustaining the case and its social impact; the influence of a specific act on a complex decision is difficult to measure; the very biases of the method used to develop this strategy could reduce this influence; and it would be relative to its media, social and political context.
3. The possible influence exerted by the micro-targeting technique used by Cambridge Analytica falls within a broader phenomenon of media manipulation bounded to new technologies and the bubble effect that has been proven to be an important reason behind the rise of online disinformation and the radicalisation of political ideas and opinions.

The Cambridge Analytica case reveals that the current development of big data technologies is generating a power inequality between citizens and a group that exercises despotic power over information and data exploitation. This affects fundamental rights like privacy, personal data protection and the right to information, as well as the democratic quality of states. For this reason, this study points out the need to:

1. Reconsider the social fitting of the structures that catalyse events like the one waged by Cambridge Analytica.
2. To not lose sight of the social and political impact of big data technologies.
3. Rethink the legal framework of personal data protection to correct its insufficiencies.
4. Establish mechanisms that allow society as a whole to have information and control mechanisms over big data technologies.
5. Impose limits, if needed, to forms of big data exploitation and/or uses that are harmful for society as a whole.

References

Alkiş, N.; Taşkaya Temizel, T. "The impact of individual differences on influence strategies. *Personality and Individual Differences, 87*(2015), 147-152. doi: 10.1016/j.paid.2015.07.037.

Baruh, L.; Popescu, M. "Big data analytics and the limits of privacy self-management". *New Media & Society*, Vol. 19, no. 4, (2015), 579-596. doi: 10.1177/1461444815614001.

Bennett, C. J. "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications". *Surveillance & Society, 13*(3/4), (2015), 370-384.<https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/voter_surv>

boyd, d.; Crawford, K. "Critical questions for big data", *Information, Communication & Society, 15*(5), (2012), 662-679. doi: 10.1080/1369118X.2012.678878.

Borgesius, F. J.; Trilling, D.; Möller, J.; Bodó, B.; de Vreese, C. H.; Helberger, N. "Should we worry about filter bubbles?" *Internet Policy Review, 5*(1), (2016). doi: 10.14763/2016.1.401.

Briant, E. L. "Pentagon Ju-Jitsu – reshaping the field of propaganda". *Critical Sociology (5 March 2018)*, 1-18. doi: 10.1177/0896920517750741.

Cadwalladr, C. "'I made Steve Bannon's psychological warfare tool': Meet the data war whistleblower". *Observer – The Guardian,* 17 March 2018. <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump> [Retrieved: 23 April 2018].

Cadwalladr, C. "The great British Brexit robbery: How our democracy was hijacked". *Observer – The Guardian*, 7 May 2017. <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy> [Retrieved: 23 April 2018].

Cadwalladr, C.; Graham-Harrison, E. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". *Observer – The Guardian*, 17 March 2018. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [Retrieved: 23 April 2018].

Cambridge Analytica. *Cambridge Analytica*. 2018. <https://cambridgeanalytica.org/> [Retrieved: 23 April 2018].

Dutton, W. H.; Reisdorf, B. C.; Dubois, E.; Blank, G. "Social Shaping of the Politics of Internet Search and Networking: Moving Beyond Filter Bubbles, Echo Chambers, and Fake News". *Quello Center Working Paper No. 2944191*. (2017), 1-26. doi: 10.2139/ssrn.2944191.

Enli, G. "Twitter as arena for the authentic outsider: exploring the social media campaigns of Trump and Clinton in the 2016 US presidential election". *European Journal of Communication*, *32*(1), (2017), 50-61. doi: 10.1177/0267323116682802.

Facebook. "¿Cómo puedo averiguar si se ha compartido mi información con Cambridge Analytica?". *Servicio de ayuda de Facebook*, 2018. <https://www.facebook.com/help/1873665312923476> [Retrieved: 18 April 2018].

Foster Shoaf, N.; Parsons, T. N. "18 Million Cracks, but No Cigar: News Media and the Campaigns of Clinton, Palin, and Bachmann". *Social Sciences, MDPI, Open Access Journal,* 5(3), (2016), 1-15. <https://ideas.repec.org/a/gam/jscscx/v5y2016i3p50-d78592.html>

Fraser, N. "Progressive Neoliberalism versus Reactionary Populism: A Choice that Feminists Should Refuse". *NORA - Nordic Journal of Feminist and Gender Research, 24*(4), (2017), 281-284. doi: 10.1080/08038740.2016.1278263.

Gaughan, A. (2016). "Explaining Donald Trump's Shock Election Win". *Scientific American*, 9 November 2016. <https://www.scientificamerican.com/article/explaining-donald-trump-s-shock-election-win/>

Grewal, P. "Suspending Cambridge Analytica and SCL Group from Facebook". *Facebook Newsroom*, 16 March 2018. <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/> [Retrieved: 18 April 2018].

Hallinan, B.; Striphas, T. "Recommended for you: The Netflix Prize and the production of algorithmic culture". *New Media & Society*, 18(1), (2016), 117–137. doi: 10.1177/1461444814538646.

Hargittai, E.; Marwick, A. "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy". *International Journal of Communication*, *10*(2016), 3737–3757.

High Level Group on Fake News and Online Disinformation. *A multi-dimensional approach to disinformation. Report of the independent High Level Group on fake news and online disinformation*. 2018. <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>. [Retrieved: 13 March 2018].

Holone, H. "The filter bubble and its effect on online personal health information". *Croatian Medical Journal, 57*(3), (2016), 298–301.

Kosinski, M.; Stillwell, D. J.; Graepel, T. "Private traits and attributes are predictable from digital records of human behavior". *Proceedings of the National Academy of Sciences of the United States of America, 110*(15), (2013), 5802-5805. doi: 10.1073/pnas.1218772110.

Marwick, A.; Lewis, R. *Media Manipulation and Disinformation Online*. *Data & Society Research Institute*, 2017. <https://datasociety.net/output/media-manipulation-and-disinfo-online/>.

Miralles-Pechuán, L.; Ponce, H.; Martínez-Villaseñor, L. "A novel methodology for optimizing display advertising campaigns using genetic algorithms". *Electronic Commerce Research and Applications*, *27*, January-February 2018, 39–51. Published online for the first time in November 2017. doi: 10.1016/j.elerap.2017.11.004.

Neumann, N. "The power of big data and algorithms for advertising and customer communication". *International Workshop on Big Data and Information Security, IWBIS 2016, art. nº 7872882*, 2017, 13-14. doi: 10.1109/IWBIS.2016.7872882.

Newman, B. I. *The Marketing Revolution in Politics: What Recent U.S. Presidential Campaigns Can Teach us about Effective Marketing*. Toronto: University of Toronto Press, 2016, 224 pages.

Nikolov, D.; Oliveira, D. F. M.; Flammini, A.; Menczer, F. "Measuring online social bubbles". *PeerJ Computer Science*, *1*(e38), (2015). doi: 10.7717/peerj-cs.38.

Oates, S.; Moe, W. W. "Donald Trump and the 'Oxygen of Publicity': Branding, Social Media, and Mass Media in the 2016 Presidential Primary Elections". *American Political Science Association Annual Meeting 2016*. doi: 10.2139/ssrn.2830195.

European Parliament. *Resolution of the European Parliament dated 14 March 2017 on fundamental rights implications of big data: privacy data protection, non-discrimination, security and law-enforcement* (2016/2225(INI)). <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//ES>

European Parliament; Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and Council, dated 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation")*. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>.

Pasquale, F. *The Black Box Society. The Secret Algorithms that Control Money and Information*. London: Harvard University Press, 2015.

Patterson, T. "News Coverage of the 2016 General Election: How the Press Failed the Voters". *Shorenstein Center on Media, Politics and Public Policy at the Harvard Kennedy School*, 7 December 2016. <https://shorensteincenter.org/news-coverage-2016-general-election/>.

Rosenberg, M.; Confessore, N.; Cadwalladr, C. "How Trump Consultants Exploited the Facebook Data of Millions". *The New York Times*, 17 March 2018. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> [Retrieved: 23 April 2018].

Sartonen, M.; Simola, P.; Timonen, J.; Lovén, L. "Cyber personalities as a target audience". *European Conference on Information Warfare and Security, ECCWS,* 2017, 411-418. <https://www.semanticscholar.org/paper/Cyber-Personalities-as-a-Target-Audience-Sartonen-Simola/1cc84c9b9ad74e426aee32828e17c54adad7246a>

Schroepfer, M. "An Update on Our Plans to Restrict Data Access on Facebook". *Facebook Newsroom*, 4 April 2018. <https://newsroom.fb.com/news/2018/04/restricting-data-access/> [Retrieved: 18 April 2018].

SCL Group. *SCL Group*. <https://sclgroup.cc/home> [Retrieved: 23 April 2018].

Shearer, E.; Gottfried, J. "News Use Across Social Media Platforms 2017". *Pew Research Centre*, 2017. <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/> [Retrieved: 23 April 2018].

Stillwell, D.J.; Kosinski, M. "myPersonality project: Example of successful utilization of online social networks for large-scale social research", *International Conference on Mobile Systems (MobiSys) 2012.* <www.michalkosinski.com/Stillwell_and_Kosinski_2012.pdf>.

Suárez-Gonzalo, S. "Big social data: límites del modelo *notice and choice* para la protección de la privacidad", *El profesional de la Información, (26)*2, (2017), 283-292. doi: 10.3145/epi.2017.mar.15.

Tufekci, Z. "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency". *Colorado Technology Law Journal (13)*, (2015), 203-218.

Turow, J.; Hennessy, M.; Draper, N. *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening them up to Exploitation*". Annenberg School for Communication University of Pennsylvania, 2015. <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>.

United States Air Force. *Psychological Operations. Air Force Doctrine Document 2-5.3. 27 August 1999*. <http://www.iwar.org.uk/psyops/resources/us/afdd2-5-3.pdf> [Retrieved: 19 April 2018].

Yingyuan, X.; Pengqiang, A. I.; Hsu, C.; Hongya, W.; Xu, J. "Time-Ordered Collaborative Filtering for News Recommendation". *China Communications, 12*(12), (2015), 53-62. doi: 10.1109/CC.2015.7385528.

Youyou, W.; Kosinski, M.; Stillwell, D. J. "Computer-based personality judgments are more accurate than those made by humans". *Proceedings of the National Academy of Sciences of the United States of America*, 112(4), (2015), 1036-1040. doi: https://doi.org/10.1073/pnas.1418680112.

Zuckerberg, M. "I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue". *Publication on Facebook*, 21 March 2018. <https://www.facebook.com/zuck/posts/10104712037900071> [Retrieved: 18 April 2018].

5

Suárez-Gonzalo, Sara [*en edición*]. Personal data are political. A feminist view on privacy and big data, *Recerca. Revista de pensament i anàlisi*.

ISSN: 1130-6149. ISSN electrónico: 2254-4135.

Artículo aceptado para publicación el día 20 de junio de 2019. Se adjuntan a continuación la carta de aceptación y la versión *pre-print*.

Universitat Pompeu Fabra Barcelona

SUAREZ GONZALO, SARA PAZ <sarapaz.suarez@upf.edu>

[RECERCA] Decisión del editor/a

Patrici Calvo Cabezas <calvop@uji.es> 20 de juny de 2019 a les 21:45
Per a: Sara Suárez-Gonzalo <sarapaz.suarez@upf.edu>

Sara Suárez-Gonzalo:

Hemos tomado una decisión sobre su envío a RECERCA. Revista de Pensament y Anàlisi, "Personal data are political. A feminist view on privacy and big data".

Nuestra decisión es: Publicable

Saludos cordiales

Patrici Calvo Cabezas
Teléfono 626604218
calvop@uji.es

Recerca. Revista de pensament i anàlisi
http://www.e-revistes.uji.es/index.php/recerca

Personal data are political. A feminist view on privacy and big data

Los datos personales son una cuestión política. Privacidad y big data en perspectiva feminista

SARA SUÁREZ-GONZALO (Universitat Pompeu Fabra)

Artículo recibido: 16 de febrero de 2019
Artículo aceptado: 20 de junio de 2019

Abstract

The second-wave feminist critique of privacy defies the liberal opposition between the public-political and the private-personal. Feminist thinkers such as Hanisch, Young or Fraser note that, according to this liberal conception, public institutions often keep asymmetric power relations between private agents away from political discussion and action. The resulting subordination of some agents to others tends, therefore, to be naturalised and redefined as a «personal problem». Drawing on these contributions, this article reviews the social and political implications of big data exploitation and questions whether personal data protection must remain a matter of «privacy self-management». It aims to show that feminist political theory can decidedly help to identify and tackle the root causes of what I call «data domination».

Key Words: big data, privacy, personal data protection, feminist theory, data domination, the personal is political.

Resumen

La crítica feminista de segunda ola a la privacidad desafía la oposición liberal entre lo público-político y lo privado-personal. Pensadoras feministas como Hanisch, Young o Fraser señalan que, de acuerdo con esta concepción liberal, las instituciones públicas a menudo dejan fuera de la discusión y la acción política las relaciones de poder asimétricas entre agentes privados. La resultante subordinación de unos agentes a otros tiende, por tanto, a ser naturalizada y redefinida como un «problema personal». Basándose en estas contribuciones, este artículo revisa las implicaciones sociales y políticas de la explotación de datos masivos y cuestiona si la protección de los datos personales debe continuar siendo una cuestión de «auto-gestión de la privacidad». Su objetivo es mostrar que la teoría política feminista puede ayudar decididamente a identificar y enfrentar las causas de lo que llamo «dominación a través de los datos».

Palabras clave: big data, datos masivos, privacidad, protección de los datos personales, teoría feminista, dominación, lo personal es político.

INTRODUCTION

Daily life is increasingly mediated by new information and communication technologies. The use of digital and online services is necessary to live a normal life in Western countries. It is unthinkable, for example, to complete a university degree or to perform certain jobs without using a computer, a mobile device or the Google search engine. Online social networks permeate social relations. Access to basic services such as health, banking or urban transport has been digitised. All this has led to a *datafication* of everyday analogue and digital life (Baruh & Popescu, 2015). The velocity, variety and volume of data generation have increased dramatically since the late 1990s, up to the point of submerging society in a «big data ecosystem» (Cox & Ellsworth, 1997; boyd & Crawford, 2011).

Our normal actions and interactions generate great amounts of personal data that spread further, faster and more broadly than ever before throughout a space controlled by private interests (Zuboff, 2019). Data can form a complex profile of our attributes, interests and preferences, but also about our environment and the persons who are part of it. In this sense, even if you do not use the services or products provided by a certain corporation, it can get information about you through the data other people generate by using those services or products, or thanks to your use of the products or services provided by related companies. By way of example, you can delete your Facebook account (or you can never have had one) and Facebook can still having information about you: this is the case of «shadow profiles» (Sarigol, García & Schweitzer, 2014). Furthermore, data disclosing is often automatic and unconscious. The case of metadata exemplifies it particularly. Due to all of this, it is very difficult, if not impossible, to actually prevent one's own life from being recorded in data (Suárez-Gonzalo, 2017).

As predicted by Lesk (2001), the velocity, variety and volume of big datasets undermine humans' capacity to make data «useful». Therefore, big data technologies draw on a new logic of data collection and analysis, which allows inferring latent information from datasets that isolated data do not reveal. At present, these techniques are necessary to decide even which of all these data deserve human attention. Furthermore, automatic mechanisms replace important human actions, as decision-making or the analysis and classification of places, objects, ideas, ways of expression and behaviours. This new «algorithmic culture» (Hallinan & Striphas, 2016) involves what, in terms of Federici (2004), would be a *mechanisation* of big data produc-

tion and reproduction. On the one side, every human activity is systematically converted in data. On the other, humans are conceived as data production machines. But, does this technological development primarily contribute to social good and equality? Or does it privilege the interests of a few?

Over the past few decades, a new business model focused on data exploitation has emerged. Data business is an opaque sector, characterised by a high business concentration that has monopolised big data turning them into a gold mine. The so-called GAFAM corporations (Google, Apple, Facebook, Amazon and Microsoft) control the data market. They gather the most of the data that billions of people disclose every day (Tufekci, 2017). As a result, both the economic value and the value for social control of the data collected by GAFAM grew exponentially. Indeed, one of their main achievements has been to start addressing data as interchangeable goods, opening the markets boundaries into them, and so paving the path for extracting profit. A practice that frames in what several authors (see Harvey, 2005; Fraser, 2016; or Arruzza, Bhattacharya & Fraser, 2019) define as a privatising, financialised and predatory form of capitalism that appropriates, rather than generates, wealth and income. Harvey (2005) uses the expression «accumulation by dispossession» to designate the mechanisms whereby this renewed expression of capitalism gets richer.

Although there are symptoms of public dissatisfaction with this situation, individuals' data-disclosing behaviours do not reflect it: people affirm to be concerned about the lack of protection of their personal data, but carry on disclosing their information in a seemingly carefree way, especially on social networks. This dissonance is known as the «privacy paradox» (Barnes, 2006). How should we interpret this apparent contradiction? Are people concerned about how big data exploitation can affect their fundamental rights to privacy and personal data protection? Are their behaviours due to ignorance, conformity or irresponsibility? Or is it perhaps a problem of impossibility to act according to the own concerns?

My point is that the privacy paradox is, primarily, a consequence of the inequality of power between citizens and those who exploit their data. While companies and corporations establish the rules for new communication and information practices, impose the data disclosing conditions through their «privacy policies», control the data flows and benefit from them; citizens generally do not have basic information about what happens

with their data, nor the means to handle the situation or to escape it. I define this asymmetric power relation as «data domination».

Following Pettit (1997; 2012), an agent (that can be an individual, a group of people or a collective or a corporation) dominates another (often individual) if he or she has a power to influence the life or decisions of the other agent that this latter does not itself control. That is what Pettit (2012) calls a power of «uncontrolled interference» (also referred to as «arbitrary interference» in Pettit's earlier works). This statement is still valid if the dominating agent is never going to make «effective» her or his power, or if the dominated agent is not aware of her or his vulnerability. In that line, Fraser (2012) holds that subordination is linked to the impossibility of detecting injustice. According to her, in a morally fair social order, everyone must have access to the same means and resources. To dominate another involves frustrating her or his possibilities to notice what is fair and unfair and/or to claim and act for justice. Thus, the lack of explicit protest should not be interpreted as an expression of justice. Combating injustice requires discursive resources and interpretative schemas that allow its identification and denounce.

It should be noted that, the monopolistic power of data markets would not be possible without the black boxed condition of the algorithmic culture. Following Pasquale (2015), corporations and governments foster an intended opacity through real and legal secrecy and obfuscation. He uses the term «agnotology» to describe the «structural production of ignorance, its diverse causes and conformations, whether brought about by neglect, forgetfulness, myopia, extinction, secrecy, or suppression» (2015: 2). This opacity reinforces people's technological disempowerment: they have the power to use technology, but not to understand it.

Facing this situation, the European legal framework for the fundamental right to personal data protection (hereinafter «PDP») –recognised by both the General Data Protection Regulation 2016/679 (hereinafter «GDPR») and the Charter of Fundamental Rights of the European Union, Art. 8 (2016/C 202/02)– is based on the liberal-hegemonic conception of privacy (Baruh & Popescu, 2015; Richardson, 2016). GDPR has been widely recognised as one of the most ambitious measures to fight personal data's vulnerability. It entails meaningful progresses in relation to the former Directive of 1995. Nonetheless, I argue in the following pages that, as feminism has shown, the liberal ideal of privacy is unable to protect people from domination. The aim of this article is to show, in light of the second wave

feminist critique of privacy, that the conceptual framework of GDPR makes it unable for citizens to protect themselves from data domination. In following this objective, the text is in two main parts: The first one focuses on the liberal-hegemonic conception of privacy that underpins GDRP. The second one explains the second-wave feminist critique of privacy and what can we learn from it in relation to data domination. Drawing on this reflection, I stand up for rethinking privacy and so personal data protection from a feminist point of view.

LIBERAL PRIVACY: AN INTERFERENCE-PROOF BUNKER

Traditionally, the private sphere has been opposed to the public one. On the one side, the public relates to the community and its concerns. Politics literally means *the things concerning the polis*. Then, preserving the public has been historically a responsibility of politics, which, at least since the Modern Age, has to do with the organisation of the government and the state. On the other side, the private refers to the personal, the domestic and property and identifies with the secret, the isolated and the hidden. Within this logic, the private has been traditionally excluded from public discussion and action, and understood as a matter of self-regulation (Mill, 1992). The limitations of this opposition between the public and the private spheres are discussed throughout the following sections.

In 1890, Warren and Brandeis famously defined the right to privacy as an extension of the right to «be let alone». A right «against the world», based on the principles of *inviolability of personality* or *immunity of the person*, and related to the protection of those aspects of life whose invasion supposes an injury to feelings. Including thoughts, emotions, unpublished productions of the intellect, sayings, acts, personal relations, domestic issues, etc. According to Warren and Brandeis, the right to privacy finishes «upon the publication of the facts by the individual, or with his consent» (1890: 8). The law, so, must have the purpose of protecting each individual from the unwarranted invasion in those private aspects with which the community has no legitimate concern.

This negative conception of privacy (as an «inviolable» sphere) is linked to liberal theory, which defines freedom as *non-interference* (see Berlin, 1969: 196 and Hobbes, 1994: 187). From the liberal perspective, a person is free if there are no interferences that modify her or his course of

action. Thus, freedom consists in doing what one wants to do, without being forced to do so. In that sense, capacity is not a condition for freedom: not having the means or the ability to do something does not mean that one is not free to do it (Pettit, 1997).

If we understand freedom as the absence of interferences between each other's actions, to be free is only possible in isolation. Because of that, several authors affirm that liberalism understands and analyses society as a sum of atomised individuals (see Bertomeu & Domènech, 2005). Hence, liberal freedom is, by definition, in conflict with social life. Nonetheless, liberal theory understands that, to guarantee that one's freedom does not harm that of others, and thus ensure other values such as security or property, living together requires the imposition of certain limits to individual freedom (Mill, 1992; Hobbes, 1994). This relates to Berlin's (1969) «value pluralism», according to which the main moral values are either equally important or incommensurable. This is a form of moral relativism that implies that there is no rational way to resolve conflicts between values. Consequently, the liberal state must refrain from promoting a certain ideal of good living. The problems of this vision have been stressed by Dworkin (2011).

In light of this theory, privacy is the individual sphere away from many of the «necessary» restrictions that life in common imposes on individuals' will when they participate in the public sphere. Liberal privacy is, let us say, a bunker of «pure» freedom, proof against interferences. The right to privacy is, then, a right to enjoy a personal sphere *exclusively* governed by the individual will.

Contemporary liberalism has criticised some aspects of this traditional way of understanding how privacy must be protected. Some of them, as Etzioni (1999) denounces that privacy has a potential to conceal actions that may threaten public order and, particularly, security. He therefore argues for reinforcing the «limits» of privacy, or, in other words, the need to restrict the «free will» in the private sphere. Solove (2008), for his part, holds that privacy is a «contextual» value that should be defined on a case-by-case individual basis, in relation to the harm (or the benefit) caused to the individual from its violation. It is up to each individual to determine which aspects of the own life he or she keeps in private or shares in public, depending on what he or she wins or loses by doing so. Regarding the protection of privacy, Solove (2013) proposes a form of «libertarian paternalism»: Taking into account the fact that people's decisions or actions to protect their private affairs are often inappropriate, he advocates replacing

individual decision by an external imposition in those cases in which this may help to keep some aspects of people's lives in private.

As seen, Both Etzioni and Solove claim for the imposition of certain limits to the individual will in the private sphere. By doing so, they nuance the traditional «inviolability» of privacy. Nevertheless, far from seeking alternative terms to redefine its value, they continue defining it in terms of interference.

Liberal privacy in GDPR

GDPR follows the *privacy self-management* paradigm (Baruh & Popescu, 2015; Solove, 2013). In other words, privacy is the underpinning value of the European PDP regulation, and there is a broad consensus that it should be so. GDPR concretises this paradigm in the *notice and choice* model (Schwartz, 2013; Solove, 2013) and establishes *individual consent* as the mechanism individuals have to protect their personal data from massive exploitation. This consent has to be *free*, *informed*, *specific* and *revocable*, and it must be expressed *clearly* and *unequivocally* (see GDPR Arts. 4(11) and 7). Hence, the interested party should notice the individual which specific data is interested in collecting or processing and for which specific purposes. The «data subject» must give her or his consent *prior to* the gathering and processing of the personal data. Nevertheless, due to the very logic of big data, it is difficult to predict which information could arise from the aggregate processing of a massive dataset. Consequently, GDPR cannot actually guarantee that individual consent is always «specific» and «informed» (Suárez-Gonzalo, 2017).

Furthermore, «free» means in the Regulation that individuals cannot be forced to share their data (see Art. 7), *i.e*., that consent must be *voluntary*. In that sense, what GDPR protects is, basically, the *inviolability* of personal data: the data-privacy of the individual in a liberal sense. On doing so, GDPR places the burden of PDP on individuals and their isolated decisions, turning consent into a sort of private, «voluntary» contract between two unequal parts: the individual and the agent that collect, analyse and use her or his data.

Nevertheless, that «contract» can be unilaterally broken in those cases related to the protection of other rights, considered equal or more important than the right to PDP. In those cases, the cession of personal data is not «free» but «necessary». These include cases in which: its processing is nec-

essary to protect the vital interest of the person; it is justified by legal obligations; for reasons of substantial public interest (including public safety and health); among others. Consent is neither required in case the data subject has disclosed them in a public space; or if the processing is carried out by an organisation not-for-profit with a political, philosophical, religious or trade union aim, provided that the processing relates solely to members or to persons who have regular contact with it and that the personal data are not shared with third parties (Article 9, d).

THE FEMINIST CRITIQUE OF THE DARK SIDE OF PRIVACY

The division of the public and the private spheres in liberal theory and practice finds some of its greatest detractors in the feminist movement. According to Pateman (1989), the public/private dichotomy is what feminist political theory is fundamentally about. The feminist movement noticed the perversity of opposing the public to the private. On the one hand, feminists pointed at a dark side of privacy that has served to hide and legitimise the domination of women. On the other, they showed how personal circumstances are structured by public factors that provoke unequal social orders. The feminist movement stressed that a person cannot be as free and equal in her or his private sphere as those to whom he or she is subordinated in the public one. Furthermore, Pateman says, feminism has devoted great efforts to investigate the contradictions of the liberal state. It brags about stopping at the threshold of the private, while configuring the private by means of laws and policies that subordinate some citizens to others due to their gender, class or race.

The personal is political

The so-called second-wave feminist movement, which arises as part of the radical socialist politics from the 60s to the 80s, was particularly concerned about the problems of the traditional public/private dichotomy. As noted by Agra Romero (2012: 35-36), second-wave feminists «defied the very unquestioned grounds of both traditional and radical politics» and stood up for a «critical review of the conventions about the limits and nature of the political and of politics». They denaturalised the power asymmetries

between men and women and redefined the limits of the 'genuinely' political.

The claim «The personal is political», popularised by a paper published by Carol Hanisch in 1970 and revisited in 2006, delves into an alternative conception of the public and the private. It came out as a reply to Dottie Zellner who criticised the actions of the Pro-Women Line faction, a specific subgroup within the radical Women's Liberation Movement in New York. The main objective of this group was to bring women's «personal problems» into the public arena, by recognizing «the need to fight male supremacy as a movement instead of blaming the individual woman for her oppression» (Hanisch, 2006: 1-2). Concerning this, Hanisch considers that individual struggle is always necessary. Even more because the oppression that affects the personal usually takes place in isolated circumstances, as the home. However, she clarifies that individual fight against oppression is limited for two main reasons: one is that when people are oppressed they act out of necessity, not out of choice; the other is that personal oppressive situations are often structured by public factors. Then, personal liberation is only possible by socially choosing to change the objective conditions of oppression, and this requires wondering about who benefits from this oppression. In other words, what Hanisch explains is that, to solve personal problems, their structural causes should be part of political discussions and actions. Otherwise, these causes become legitimate.

In this respect, Federici's (2004) work is enlightening. It focuses on the historical subordination of women to men and to the «domestic» (or the private). Federici argues that this is not a causal relation, but the result of the transformations of gender relations prompted by early capitalist forms of accumulation that turn the female body into a means for the «re»production of labour.

In line with this, Nancy Fraser (2012) defends the importance of questioning the liberal tendency to redefine structural inequities as personal problems. She expounds the need to investigate the reasons behind those interpretations that attribute people's unfavourable circumstances to their own weaknesses. Instead of looking for individual panaceas to the problems that affect all of us, Fraser advocates examining biases of the public sphere that expose some persons to different moral considerations that impede their equal access to the political voice.

The feminist movement has interpreted Hanisch' claim in various ways. Some have supported the elimination of privacy. Others, its imposition:

According to MacKinnon (1989), the right to privacy has failed to protect women's inviolability. The public/private split has left the private domain out of any form of public scrutiny. Because of that, privacy has become closer to a right to impunity of those men who dominated, oppressed and degraded women, than a right to inviolability of the dominated. In MacKinnon's words (1989: 191), «For women, the measure of the intimacy has been the measure of the oppression». In that light, she holds that feminism has to «explode» the private.

For her part, Young (1987) defends that the determination of privacy must remain. She defines privacy as that aspect of the life and activity that any individual has a right to exclude others from, instead of understanding it as what is excluded from the public. In Young's view, «the personal is political» does not imply denying the distinction between public and private spheres in itself, but the social division that their opposition leads to. The unified model of individuality that has been traditionally imposed in public life discriminates those who do not meet the average canons. It has set aside some persons from the public life by condemning some of their personal attributes or actions to remain private. Her proposal elaborates on a «heterogeneous» ideal of public life which recognises and appreciates the differences, instead of excluding them. Thereby, Young considers that, the defence of privacy «has become not merely a matter of keeping the state out of certain affairs, but asking for positive state action to ensure that the activities of nonstate organizations, such as corporations, respect the claims of individuals to privacy» (1987: 74). In this way, she recognises two principles following from Hanisch's claim: «(a) no social institutions or practices should be excluded a priori as being the proper subject for public discussion and expression; and (b) no persons, actions or aspects of a person's life should be forced into privacy.»

Contrarily to Young, and similarly to Solove's (2013) libertarian paternalism, Allen (1999) advocates the need to «coerce privacy». A whole lifestyle premised on disclosure ought not to be an option. Therefore, she stands up for externally imposing individuals to keep some aspects of their lives in private. According to Allen, due to contemporary cumulative damages to privacy –particularly generated by new technologies–, people have «an ethical obligation to protect their own privacy». Then, they have to be forced «to have private lives and to live their private lives in private» (1999: 752). Allen (2016) understands the protection of privacy as a ethical responsibility shared by governments, businesses, and individuals. In her view, the

role of a good government has to be to protect some forms of privacy that individuals do not value.

To sum up, while Young's interpretation of the claim proposes an alternative conception of privacy to the liberal one, MacKinnon and Allen do not actually move away from privacy's «inviolable» conception.

FEMINISM FOR PERSONAL DATA PROTECTION

The feminist struggles arise as a reaction to the historical subordination of women to men. The objective of feminist theory is to analyse the causes of this subordination and reverse them. It is precisely with the aim of putting an end to women's inferiority of power that feminism brings to light the problems of privacy.

Feminism, maintains Agra Romero (2012), is politics and is political theory. The experience of women has not only influenced and provoked changes at a personal and social level, but also at a theoretical level that pushes for re-examining the domains of the political, and questioning the conventional opposition of the public and the private spheres. Then, feminism should not be reduced to an ideology or a movement.

Following Federici (2004: 13), feminist political theory has confirmed that «to look at history from a feminist viewpoint means to redefine in fundamental ways the accepted historical categories and to make visible hidden structures of domination and exploitation».

«The personal is political» (Hanisch, 1970; 2006) expresses the need to overcome the liberal dualism in which the personal becomes depoliticised. It notes that this division leads to an exclusion of the problems that affect the personal from political discussion and action. The claim denounces the inability of privacy to prevent situations of domination in the private sphere, by keeping out of public scrutiny the impunity of those who dominate. It also draws attention to the liberal tendency to look at social life exclusively in personal terms, and alerts about the importance of political actions to overcome domination in the personal sphere.

Furthermore, a large part of feminist studies (Fraser, 2012; Hanisch, 1970; Pateman, 1989; Young, 1987) understand that overcoming the depoliticisation of the personal implies pursuing a different social order, based on a social conception of individuality within which public and private di-

mensions are distinguished, but not opposed. With regards to this, García Manrique (2013), points out the importance of feminist's contributions to the terms in which private life must be sustained by a politically organised community. He notes that, although politics should not have to establish the conditions of the private life, it must become aware that the private sphere depends on publicly imposed conditions. And also that freedom depends, too, on the conditions of the private life. Thus, the political community should not ignore private life, but rather it should enable and promote the conditions so that the private life can also contribute to everyone being equally free.

These analysis and conclusions of the feminist critique of privacy are, from my point of view, applicable to other situations of inequality comparable to those that cause the subordination of women. I mean here to emphasise that the theoretical outcomes of the feminist movement are not only applicable to women's struggles, but also to diverse critical analysis of unequal social structures. As regard to this, the claim «the personal is political» may be, in my view, very illuminating to rethink PDP regulations. It shows us that the solution to the personal vulnerabilities caused by personal data's massive exploitation cannot be restricted to isolated action. Moreover, that, even if the «agreement» between the citizen and a certain company that uses her or his data is a «private» relationship, the protection of personal data should be excluded from public scrutiny.

In that light, equating the right to PDP with the inviolability of personal data blocks the possibilities of tackling the root causes of data domination. By establishing individual consent as the only mechanism citizens have to protect their data, GDPR confines people to individual resistance facing highly concentrated and organised markets, whose use of big data affects the personal affairs of all of us. On doing so, the Regulation cuts off the possibilities of giving a socially organised response to the implications of big data exploitation. In that sense, GDPR replaces social protection by what Harvey (2005) calls a «personal responsibility system». A system devoid of democratic control where individual cessions shape the type of society where we all live. Besides, it confers the market the status of «appropriate guide» for the development of big data technologies. Within this situation, people's options restrict to two: to trust the markets' goodwill; or to act as technophobes, trying to marginalise their own actions and beliefs from data accumulation. This situation entails the risk of entering pri-

vacy into a game of preferences that excludes those who do not share the rules imposed by data business.

Arruzza, Bhattacharya and Fraser (2019: 50) note that the effect of this system, rooted in the institutional structure of capitalism, «is to declare vast swaths of social life off limits to democratic control and turn them over to direct corporate domination». It fails to fulfil the supposed role of public institutions in contemporary welfare states: to replace the logic of the markets by an equal distribution of goods, through the recognition of a set of legal rights to all members of a political community (Marshall, 1950). On these grounds, it seems clear that we should not seek protection for personal data in darkness, secrecy and from the isolation. Rather, the answer must be, also, political. Moreover, feminism lays bare the need of protecting the personal from the subordination of the individual will, instead than only from its interference.

CHANGING PERSPECTIVE

In my view, the dark side of privacy is a consequence of defining its value in terms of (absence of) interferences. Within this framework, to ensure privacy consists of building walls around the private and the personal to guard it from external interferences, but not from subordination. In the case of PDP, the role of the state restricts to guaranteeing the «self-management» of personal data. That is, that no one could force or prohibit another to consent the unwarranted publication, gathering or use of her or his data. Privacy in that sense lacks aspirations for equality in the private sphere by leaving outside its scope of protection the inequalities of power affecting private relations. This applies not only to the traditional conception of privacy, but also to some of its critics, such as Etzioni (1999), Solove (2003) or Allen (1999), who do not move significantly away from the definition of privacy in terms of non-interference.

Do these weaknesses of the liberal model of privacy mean that privacy is not a suitable value for underpinning PDP regulations? Should they lead us to forget the distinction between the public and the private? Certainly not. As I understand privacy, it is a sphere where we enjoy our freedom in a particularly individualised way. Therefore, the idea of freedom we refer to determines the way we understand privacy and the protection of the private-

personal. This idea has been also noted by Roberts (2018: 6): «re-examining the beliefs that we hold about the nature of freedom –its constituent conditions– might, if it causes a shift in those beliefs, lead us to think differently about privacy».

Consequently, my proposal is not to reject or to restrict privacy as the articulating value of PDP regulations, nor to reject or to restrict individual decision as the main mechanism to protect personal data. Rather, it seems necessary to defy the liberal hegemonic conception of privacy by rethinking its value from an alternative conception of freedom.

The aim of this article is not to delve deeper into this issue. Even though, in the following lines I sketch out that a neo-republican conception of privacy would overcome the problems of liberal privacy, and so, it would be may be more suitable for protecting people from data domination.

Neo-republicanism defines freedom as *non-domination* (Pettit, 1997; 2012). The main difference between liberal and republican freedom lies in the type of hindrances that they consider inimical to freedom. While liberalism considers that there go against freedom all the interferences that modify the individual will that guide a course of action; republicanism understands that a person is not free if he or she is exposed to another's uncontrolled power of interference. Whether if this power affect *directly* or *indirectly* the individual capability of choosing a valuable course of action and carrying it out, and whether this power is actually *exercised* or just *potential*. By way of explanation, an agent may dominate another without actively interfering in any of her or his actions, as well as it is possible to interfere in the actions of an agent without dominating him or her. In that line, Pettit notes that dominating relationships can have their origin in consent in case it gives one party the uncontrolled capacity to influence the life of the other. Therefore, republicanism recognises the importance of power relations when thinking about freedom. Contrarily to liberal freedom, republican freedom tends to social equity. This implies that preventing one agent from dominating another is a way of ensuring the freedom of all, and not a form of limiting it.

To be free in the republican sense means to not being exposed to any power of interference that one cannot autonomously control. In that sense, freedom requires a series of material and immaterial conditions that must be equally accessible by every citizen. The role of public powers is then to protect and resource citizens against domination, provided that this action of the state responds to the mandate of the citizenry (Pettit, 2012).

Bertomeu and Domènech (2005) note that «X is strengthened in his civic-political freedom by a more or less large core of constitutive (not purely instrumental) rights that no one can take away from him, nor can he himself alienate (sell or donate) at will, without losing his status of free citizen.» (our transl.). From this perspective, the liberal dichotomies between freedom and other goods or the public interest, lose their meaning, since relationships between rights become a matter of reciprocal necessity.

Drawing on republican theory, privacy would be closer to a sphere free from arbitrary interferences in order to ensure individual's will concerning private and personal issues, but also her or his ability and means to carry out such will. Privacy would still be a sphere governed by the individual will, shared with the subjects that the person wants and where the individual does what he or she wants to do. But, at the same time, it would allow to guard the individual from isolation when facing situations of oppression at a personal level. Contrarily to liberal privacy, republican privacy would protect the individual not only from violations of her or his individual will regarding private issues, but also from the subordination to others' wills.

CONCLUSIONS

Privacy is a distinctive value of liberalism. It underpins the European legal framework for PDP.

From the lens of liberal theory, privacy is an «inviolable» sphere proof against others' interferences. Ensuring privacy means guarding the individual against the injury inflicted by invasions upon her or his personal affairs. This conception of privacy is unable to protect the individual from the subordination of her or his will, as feminism has shown.

The second-wave feminist claim «the personal is political» pushes for critically examining the traditional opposition between public and private spheres. Feminist theory notes that asymmetric power relations between "private agents" give rise to the oppression of the less powerful agent. By keeping the causes of these inequalities away from public discussion and action, public institutions tend to naturalise the resulting subordination of ones to others and to redefine it as a «personal problem». A clear example is the historical subordination of women to men. On doing so, politics relegates the resolution of these problems to individual fights, complicating to tackle their root causes as a society.

Beyond being a key element in women's struggles, this feminist critique of privacy represents a substantial contribution in theoretical terms. This article shows that it is an illuminating approach to reviewing the meaning and scope of PDP regulations. Looking at PDP from a feminist point of view means: Firstly, to redefine the inviolable conception of privacy that underpins GDPR in order to overcome the depoliticisation of personal data protection. Secondly, to make visible the hidden structures of domination behind the massive exploitation of personal data. Thirdly, to stop thinking that individual action is the only way to freely protect personal data. Society has to use its ability to decide collectively which would be the best way to protect personal data.

Keeping this in mind, my proposal is not to reject or to restrict privacy as the articulating value of PDP regulations. I stand up for defying the liberal conception of privacy in light of the republican conception of freedom as non-domination and so, recognizing the social dimension of the right to PDP. This does not mean one has to force people to keep hidden their personal data, nor to take decisions about the protection of their data in a particular sense. It is about to ensure that individual decisions regarding private issues are not (directly or indirectly) subordinated to others' interests. Consequently, it is critical to reduce the factors that give a few corporations the power to undermine citizens' ability to act autonomously for the protection of their personal data.

This requires that public institutions replace the logic of data business for the logic of fundamental rights, limiting the unbridled expansion of the markets to data. It is essential to promote the widest possible public debate on the development of big data technologies and personal data protection regulations, even questioning its conceptual foundations. Public institution should support this debate by providing mechanisms of transparency, external control and accountability of big data technologies and data-driven corporations. All this would legitimate political actions to ensure everyone's possibilities to detect and protest against unfair big data exploitation practices, and to take free decisions about their personal data away from the pressures of data business.

ACKNOWLEDGMENTS

I would like to thank the organiser and participants of the «Value of Privacy» track at the Amsterdam Privacy Conference 2018 for their comments and questions on an earlier draft of this article.

REFERENCES

Agra Romero, María Xosé (2012). El feminismo y/en la filosofía política. *Laguna. Revista de Filosofía, 30*, 31-45. Retrieved from: http://riull.ull.es/xmlui/handle/915/2450.

Arruzza, Cinzia; Bhattacharya, Tithi and Fraser, Nancy (2019). *Feminism for the 99%. A manifesto*. London, Brooklyn: Verso, New Left Books.

Allen, Anita L. (1999). Coercing Privacy. *Faculty Scholarship. Paper 803*. Retrieved from: https://scholarship.law.upenn.edu/faculty_scholarship/803.

Allen, Anita L. (2006). Protecting One's Own Privacy in a Big Data Economy. U of Penn Law School, Public Law Research Paper No. 17-1. *Harvard Law Review Forum, 130*, 71-78. Retrieved from: http://ssrn.com/abstract=2894545.

Barnes, Susan B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9), 1-10. doi: https://doi.org/10.5210/fm.v11i9.1394.

Baruh, Lemi and Popescu, Mihaela (2015). Big data analytics and the limits of privacy self-management. *New media & Society*, 1-18. doi: https://doi.org/10.1177/1461444815614001.

Berlin, Isaiah (1969). *Four Essays On Liberty*. Oxford, England: Oxford University Press.

Bertomeu, María-Julia and Domènech, Antoni (2005). El republicanismo y la crisis del rawlsismo metodológico (Nota sobre método y sustancia normativa en el debate republicano). *Isegoría, 33*, 51-75. doi: https://doi.org/10.3989/isegoria.2005.i33.418.

Bobbio, Norberto (2009). *Igualdad y libertad*. Barcelona: Ediciones Paidós Ibérica SA.

boyd, danah and Crawford, Kate (2011). Six provocations for big data. *Paper presented at: A decade in internet time: Symposium on the dynamics*

of the internet and society, Oxford Internet Institute. doi: http://dx.doi.org/10.2139/ssrn.1926431.

Charter of Fundamental Rights of the European Union (2016/C 202/02). Retrieved from: http://data.europa.eu/eli/treaty/char_2016/oj.

Cox, Michael and Ellsworth, David (1997). *Application controlled demand paging for out-of-core visualization. Report NAS-97-010, July 1997.* Moffet Field: NASA Ames Research Centre. Retrieved from: https://www.nas.nasa.gov/assets/pdf/techreports/1997/nas-97-010.pdf.

Dworkin, Ronald (2011). *Justice for hedgehogs*. Cambridge, London: Harvard University Press.

Etzioni, Amitai (1999). *The limits of privacy*. New York: Basic Books.

Federici, Silvia (2004). *Caliban and the witch. Women, the body and primitive accumulation*. Brooklyn: Autonomedia.

Fraser, Nancy (2012). On justice. Lessons from Plato, Rawls and Ishiguro. *New Left Review 74*, March-April 2012. Retrieved from: https://newleftreview.org/II/74/nancy-fraser-on-justice.

Fraser, Nancy (2016). Progressive Neoliberalism versus Reactionary Populism: A choice that feminists should refuse. *NORA – Nordic Journal of Feminist and Gender Research, 24*(4), 281-284. doi: http://dx.doi.org/10.1080/08038740.2016.1278263.

García Manrique, Ricardo (2013). *La libertad de todos. Una defensa de los derechos sociales.* Barcelona: El Viejo Topo.

Hallinan, Blake and Striphas, Ted (2016). Recommended for you: The Netflix Prize and the production of algorithmic culture. *New Media and Society, 18*(1), 117-137. doi: https://doi.org/10.1177/1461444814538646.

Hanisch, Carol (1970). The personal is political, *Notes From the Second Year: Women's Liberation. Major Writings of the Radical Feminists*, 76-78.

Hanisch, Carol (2006). The personal is political. The Women's Liberation Movement classic with a new explanatory introduction. *Women of the World, Unite! Writing by Carol Hanisch.* Retrieved from: http://www.carolhanisch.org/CHwritings/PIP.html.

Harvey, David (2005). *A brief history of Neoliberalism*. New York: Oxford University Press.

Hobbes, Thomas (1994). *Leviathan*. [Edited with Introduction and Notes by Edwin Curley]. Indianapolis: Hackett.

Laney, Douglas (2001). *3D data management: Controlling data, volume, velocity and variety, Application delivery strategies*, *File 949.* Meta Group Research Note. Retrieved from: https://blogs.gartner.com/doug-

laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Lesk, Michael (1997). *How Much Information Is There In the World?* Retrieved from: http://www.lesk.com/mlesk/ksg97/ksg.html.

MacKinnon, Catharine (1989). *Toward a Feminist Theory of the State*. Cambridge: Harvard University Press

Marshall, Thomas H. (1950). *Citizenship and social class*. Cambridge: Cambridge University Press.

Mill, John Stuart (1992). *On liberty and other essays*. [Edited with Introduction by John Gray]. New York: Oxford University Press.

Pasquale, Frank (2015). *The black box society. The secret algorithms that control money and information*. Cambridge: Harvard University Press.

Pateman, Carole (1989). *The Disorder of Women: Democracy, Feminism, and Political Theory*. Stanford: Stanford University Press.

Pettit, Philip (1997). *Republicanism. A theory of freedom and government*. Oxford: Oxford University Press.

Pettit, Philip (2012). On the people's terms. *A Republican Theory and Model of Democracy*. New York: Cambridge University Press.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Retrieved from: http://data.europa.eu/eli/reg/2016/679/oj.

Richardson, Janice (2016). *Law and the philosophy of privacy*. London: Routledge.

Roberts, Andrew (2018). Why privacy and domination? *European Data Protection Law Review, 1(4), 5-11. doi: 10.21552/edpl/2018/1/4.*

Sarigol, Emre; Garcia, David y Schweitzer, Frank (2014). Online Privacy as a Collective Phenomenon. *COSN '14 Proceedings of the second ACM conference on Online social networks*, 95-106. doi: https://doi.org/10.1145/2660460.2660470.

Schwartz, Paul M. (2013). The EU-US privacy collision: A turn to institutions and procedures. *Harvard law review, (126)*7, 1966-2009. Retrieved from: http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_schwartz.pdf.

Shalev-Shwartz, Shai and Ben-David, Shai (2014). *Understanding Machine Learning: From theory to Algorithms*. New York: Cambridge University Press.

Solove, Daniel J. (2008). *Understanding privacy*. Cambridge: Harvard University Press.

Solove, Daniel J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard law review, (126)*7, 1880-1903. Retrieved from: http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf.

Suárez-Gonzalo, Sara (2017). Big social data: Some limitations of notice and choice for privacy protection. *El Profesional de la Información, 26*(2), 283-292. doi: https://doi.org/10.3145/epi.2017.mar.15.

Tufekci, Zeynep (2015). Big questions for social media big data: Representativeness, validity and other methodological pitfalls. *Procedings of the 8th Intl AAAI Conferece on weblogs and social media.* Retrieved from: https://arxiv.org/abs/1403.7400.

Tufekci, Zeynep (2017). *Twitter and the tear gas. The power and fragility of networked protest*. New Haven and London: Yale University Press.

Warren, Samuel D. and Brandeis, Louis D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. doi: 10.2307/1321160.

Young, Iris Marion (1987). 'Impartiality and the Civic Public', in: Benhabib, Seyla and Cornell, Drucilla (eds.) (1987). *Feminism as Critique. On the politics of Gender*. Minneapolis: University of Minnesota Press.

Zuboff, Shoshana (2019). *The age of surveillance capitalism. The fight for a human future and the new frontier of power*. New York: Public Affairs.

Difusión de resultados

Congresos internacionales

Los resultados de esta tesis se han presentado en cuatro congresos internacionales celebrados en España y los Países Bajos:

1. Suárez-Gonzalo, Sara (10 de marzo de 2016). Desafíos y oportunidades de la implementación de la analítica Big Data a la actividad publicitaria, *Simposio 5: ¿El regreso de Prometeo?: Algoritmos y big data desvelan el misterio de la comunicación política. I Congreso Internacional Comunicación y Pensamiento "Comunicracia y Desarrollo Social"*. Universidad de Sevilla.

2. Suárez-Gonzalo, Sara (14 de septiembre de 2017). Big Data, automatismo y opacidad: límites para la privacidad y la libertad individual, *Sección temática 4: Filosofía, ciencia, tecnología y sociedad. II Congreso de la Red Española de Filosofía: Las Fronteras de la Humanidad*. Universidad de Zaragoza.

3. Suárez-Gonzalo, Sara (5 de octubre de 2018). Sobre la mercantilización de lo personal: propiedad, cuerpo y datos masivos, *XIX Semana de Ética y Filosofía Política. Congreso Internacional de la Asociación Española de Ética y Filosofía Política (AEEFP) y la Sociedad Iberoamericana de Estudios Utilitaristas (SIEU). Ferrol 2018, "Nuevas narrativas éticas y políticas*". Universidade de A Coruña.

   De la participación en este congreso se extrae la siguiente publicación, vinculada a la tesis:

   Suárez-Gonzalo, Sara [*en edición*]. Sobre la mercantilización de lo personal: propiedad, cuerpo y datos masivos, *e-Actas XIX Semana de Ética y Filosofía Política Congreso Internacional AEEFP-SIEU. Nuevas Narrativas éticas y políticas*. A Coruña: Sociedad Iberoamericana de Estudios Utilitaristas (SIEU).[11]

4. Suárez-Gonzalo, Sara (6 de octubre de 2018). Understanding republican privacy for personal data protection, *Value of Privacy Track. Amsterdam Privacy Conference 2018.* Amsterdam Platform for Privacy Research (APPR), University of Amsterdam.

[11] El ISBN de esta publicación, todavía en proceso de edición, es el siguiente: 978-84-09-04968-4. Esta información ha sido proporcionada mediante un correo electrónico de aceptación emitido el 27 de junio de 2019 por José Luis Tasset Carmona, presidente del comité organizador del congreso.

Seminarios impartidos

Además, se han impartido tres seminarios, dos de ellos invitada por grupos de investigación de otras universidades:

1. Suárez-Gonzalo, Sara (16 de marzo 2017). Procesamiento big data y límites para la autogestión de la privacidad, *Taula de Nova Recerca*. Departament de Comunicació, Universitat Pompeu Fabra.

2. Suárez-Gonzalo, Sara (29 de noviembre de 2017). Sobre la paradoja de la privacidad y la explotación de datos masivos, *Seminario del Barcelona Science and Technology Studies Research Group (STS-b)*. Departamento de Psicología Social, Universitat Autònoma de Barcelona.

3. Suárez-Gonzalo, Sara (15 de mayo de 2019). Privacy, freedom and the socio-political implications of big data technologies, *Ethics and Politics of Emerging Technologies Meeting (MEPET)*. Department of Philosophy, Maastricht University.

   Este seminario fue organizado como parte de una estancia de investigación realizada durante la primavera de 2019 en el Science, Technology and Society Studies (MUSTS) Research Group, vinculado al Departamento de Filosofía de la Maastricht University.

   La estancia fue dirigida por el Prof. Dr. Tsjalling E. Swierstra y financiada por el YERUN Research Mobility Award 2018-2019, un premio europeo concedido por la Young European Research Universities Network a parte de la investigación realizada en esta tesis.

Discusión: el impacto de la explotación big data

Los diferentes apartados de esta memoria y las cinco publicaciones del compendio han definido las características centrales de la lógica de generación, recopilación y procesamiento de datos masivos [**OE1**]; las dinámicas del modelo de negocio de los gigantes digitales [**OE2**]; los elementos y los actores principales del discurso mediático mayoritario sobre las tecnologías big data [**OE3**]; las reacciones sociales y las formas de resistencia promovidas por los sectores especializados [**OE4**]; y el modelo de protección de datos en Europa, incluyendo su fundamentación teórica y conceptual [**OE5**].

Asimismo, las publicaciones han contribuido a interpretar en qué medida el contexto general en el que se produce la explotación de datos masivos favorece u obstaculiza la privacidad y la libertad de las personas, así como su control sobre los datos [**OG2**]. En particular, se han focalizado más el impacto de las lógicas big data [**OG2–OE1**] y el modelo de negocio de las grandes compañías explotadoras de datos [**OG2–OE2**], y en evaluar la eficacia o la pertinencia del marco jurídico europeo para hacer frente a este impacto [**OG2–OE5**].

Este capítulo organiza y relaciona algunas de las aportaciones más importantes de los artículos y las interpreta de una forma conjunta, con el propósito de dar pleno cumplimiento al objetivo general 2. No se propone abordarlas de forma exhaustiva, sino resaltar sus aspectos más destacados y explicitar algunas cuestiones que han tenido que quedar fuera de los artículos publicados.

Se divide en cinco secciones. Cada una de ellas relaciona el [**OG2**] con los cinco contextos analizados.

[OG2–OE1] Un big data incontrolable

Esta sección señala los factores relativos a la lógica de generación, recopilación y procesamiento de datos masivos de mayor interés para el OG2:

Atrapados en los datos

Los productos y los servicios digitales (o digitalizados) son necesarios para la vida moderna. En el presente es prácticamente imposible vivir una vida común en el mundo occidental sin utilizar productos o servicios de las grandes corporaciones tecnológicas.

Esta digitalización ha contribuido a conformar un escenario de *datificación* masiva, en el cual son tantas las acciones y comportamientos ordinarios que se registran en forma de datos, que es complicado que una persona pueda ser plenamente consciente de qué y cuánta información difunde en su vida cotidiana.

Los datos generados pueden referirse a uno mismo, a las características y las personas de su entorno, o a otras personas. Así, aunque la persona sea consciente de qué y cuánta información difunde, puede que las otras personas a las que también se refiere esa información no lo sean. Por tanto, la datificación presenta dos primeros problemas:

- La difusión de información personal puede ser inconsciente y no es exclusivamente personal.

En el caso de que todas las personas a las que se refieren los datos generados fueran perfectamente conscientes de qué y cuántos datos difunden mediante sus acciones y comportamientos cotidianos, podrían estar satisfechas con ello, o no estarlo. En el segundo caso, podría no estar en su mano dejar de realizar esas acciones, a fin de evitar esa difusión de información, o su vida podría verse significativamente afectada al hacerlo.

- La difusión de datos puede resultar inevitable.

Dado que estas dinámicas afectan a todas las personas, los datos generados no sólo sirven para definir a una persona, sino también a un "tipo de persona", a una persona como parte de un grupo o un entorno, al grupo en sí mismo o respecto a otros grupos, o al entorno en sí mismo o en relación a otros entornos, etc.

- La difusión de datos tiene un impacto social.

En consecuencia, conseguir que no se genere o difunda información sobre uno mismo no está en la mano de esa persona. Llevándolo al extremo, sólo sería posible si todas las personas relacionadas de alguna manera directa o indirecta con uno mismo dejasen de difundir información.

Tendencia al descontrol

Por otra parte, dado que la recopilación de los datos es masiva e indiscriminada, se recogen todo tipo de datos, independientemente de su estructura, su fuente de procedencia y su contenido. La cantidad de información es tal que son la criba y el procesamiento realizados *a posteriori*, los que determinan qué información emerge de los datos recogidos.

- Es complicado, tanto para la persona que difunde información como para quien la recoge, prever qué información, cuánta y de qué tipo se obtendrá.

Además, las técnicas de procesamiento agregado de los datos permiten extraer información sensible de datos que, aislados, eran aparentemente irrelevantes.

- Así, es complicado determinar qué datos deben considerarse "personales" o "sensibles". Especialmente si se evalúan por separado y previamente a su tratamiento.

Por último, la magnitud de los datos masivos y la complejidad y la opacidad de las técnicas de generación, recopilación y procesamiento impiden el control y la supervisión humana de los procesos. Su consecuente automatización y la cantidad de actores involucrados dificultan la posibilidad de identificar al agente responsable del proceso y el encargado de rendir cuentas por sus consecuencias.

- Como resultado, los sistemas basados en el análisis autónomo de datos masivos, como es el caso de las técnicas de aprendizaje de máquinas, son muchas veces ininteligibles e imprevisibles, incluso para sus propios desarrolladores.

De todo lo anterior pueden extraerse cuatro tesis relevantes sobre el impacto de la lógica big data en la privacidad, la libertad y el control de datos:

1. Es cada vez más complicado permanecer al margen de la datificación, en dos sentidos: a) dejar de contribuir a generar datos y, b) mantener la propia vida *indatificada*.
2. El impacto de la explotación de datos masivos y su control trascienden el nivel personal. Se produce en red y afectan al conjunto de la sociedad.
3. Es difícil determinar, de forma aislada y previa a la recopilación y al tratamiento, qué información se obtendrá de los datos y, por tanto, qué es *un* dato personal.
4. Los procesos de generación, recopilación y procesamiento de los datos tienden a ser cada vez menos previsibles y controlables por los humanos.

[OG2–OE2] En las manos de unos pocos

Esta sección se centra en el impacto del modelo de negocio de las grandes corporaciones tecnológicas:

La mercantilización de los datos

La principal fuente de financiación de corporaciones como Google o Facebook proviene de la explotación comercial de los datos que los individuos generan al interactuar con sus productos y servicios. Por ello, estas empresas han comenzado a tratar los datos como un nuevo bien de mercado, del cual los individuos disponen y pueden transferir. Es una actuación propia de un sistema capitalista cada vez más preocupado por la especulación y la privatización, que se apropia de la riqueza, pero apenas la produce.

La inercia del monopolio

Los *efectos de red* [8] hacen que estas grandes corporaciones tecnológicas concentren los servicios y productos más utilizados en su sector. Esto obstaculiza la competencia del mercado y dificulta que los ciudadanos puedan elegir fácilmente dejar de cederles sus datos. En consecuencia, estas empresas recopilan la mayoría de los datos que se generan en el entorno digital.

[8] Véase la página 16.

Otro punto central para su éxito es conseguir que sus sistemas predominen con respecto al de las empresas de la competencia. La propiedad de las innovaciones en los métodos de generación, recopilación y análisis de los datos se concentra también, y de forma opaca, en estas grandes empresas.

Por otra parte, el creciente peso que estas corporaciones han alcanzado en la economía global, y el potencial de los datos que recopilan para el control social, les ha situado en una posición favorable con respecto a los poderes públicos, que les permite ejercer fuertes presiones sobre las políticas impositivas y las regulaciones nacionales e internacionales.

Estas cuestiones ponen de manifiesto que, en la práctica, los efectos de la lógica big data [OG2–OE1] y los del modelo de negocio de las grandes corporaciones tecnológicas de servicios digitales [OG2–OE2], son indisociables.

Más concretamente, y como continuación de las primeras cuatro aportaciones:

5. La concentración de poder de las grandes corporaciones tecnológicas complica la capacidad de los individuos y de las instituciones para ejercer una influencia significativa sobre los procesos de explotación de los datos que estas llevan a cabo.
6. Los efectos de la lógica big data (puntos 1 a 4) son particularmente operativos para el beneficio económico de los *gigantes digitales*.
    a) Respecto al punto 1: la dificultad para mantenerse al margen de la datificación contribuye al monopolio de las grandes corporaciones digitales.
    b) Respecto al punto 2: el impacto conectado y social de la lógica big data se traduce en una extensión del ámbito de influencia de las grandes corporaciones, que no solo afecta a las personas usuarias de sus productos y servicios.
    c) Respecto al punto 3: existe una gran dificultad para conocer de qué información disponen en la práctica estas empresas y cómo la utilizan.
    d) Respecto al punto 4: la tendencia al descontrol de las tecnologías de procesamiento de datos masivos beneficia al modelo de negocio de estas grandes empresas. Cuánto más imprevisibles, fragmentados y opacos sean los procesos internos de tratamiento de los datos, más complicado será

comprenderlos o evaluarlos de forma externa, atribuir responsabilidades por los resultados de los mismos y demandar que se rindan cuentas por ellos.

7. Como resultado de la centralidad de los productos y servicios de estas empresas en la sociedad moderna, la capacidad individual para dar una respuesta diferente (por ejemplo, dejar de usarlos) a la mayoritaria, se reduce. Por tanto, no podemos considerar que sea una elección verdaderamente "libre" dejar de proporcionales datos.
8. La posición de superioridad que estas grandes multinacionales han alcanzado les permite presionar la acción de los poderes democráticos en favor de políticas adecuadas a sus intereses.

[OG2–OE3] Un discurso sesgado

La tesis se ha aproximado al discurso dominante sobre las tecnologías big data mediante la revisión bibliográfica de estudios previos y la realización de dos análisis empíricos exploratorios[9]. Este análisis también permite extraer algunas conclusiones relativas al objetivo general 2.

En primer lugar, mediante los estudios realizados se ha observado que el discurso mediático dominante sobre las tecnologías big data confirma las tendencias señaladas por estudios previos con respecto a la tecnología digital o de la computación.

Elementos interpretativos y discursivos

En cuanto a los elementos del discurso, el análisis realizado sobre big data en Twitter muestra que los términos más frecuentes (*analytics/analysis*, *you/your*, *how*, marketing/market, *cloud*, *business*, *will*, *use*, *can*, *predict*, *what*, *Hadoop*, *IBM*, *help*, *why*, *company*, *future*, *next*, *social*, *world*…) y los mensaje más influyentes: a) vinculan los datos masivos con una realidad inmaterial; b) promueven una concepción pragmática y utilitarista de los datos, muy centrada en mundo de los negocios y el marketing; c) se centran en las posibilidades futuras del análisis de datos. Por otra parte, es llamativo que el segundo término más utilizado en las intervenciones sea *you/yours*

[9] Véanse el artículo 1, en la página 53 y el artículo 2, en la página 75.

(en castellano *tú*/*tuyo*/*tuyos*), con una frecuencia de 9.642 apariciones. Esto pone de manifiesto que el discurso sobre big data apela al lector de forma directa, ya sea como individuo particular, ya sea para hacer referencia a *algo* que le pertenece.

El análisis sobre el caso Tay muestra que el marco interpretativo dominante (*F.5. Atribución de responsabilidad*) se centra en culpar del funcionamiento indeseable del *chatbot* (reproducción de un discurso racista y homófobo) a las personas que interactúan con él, fomentando la idea de que los efectos de la tecnología se derivan del uso individual que las personas hacen de ella. Un marco que, según Semetko y Valkenburg (2000), alienta a la opinión pública a solventar los problemas sociales que esta cause en el plano individual. En cuanto a la descripción de la tecnología, el lenguaje utilizado es vago e impreciso: recurre a elementos emocionales, tiende al uso de la metáfora y la personificación (fundamentalmente se refiere al chatbot como un "bebé" víctima de un "ataque organizado") y aporta explicaciones sesgadas y descontextualizadas sobre su funcionamiento. Apenas se habla de ello desde un punto de vista técnico o científico. El caso se presenta como un evento aislado, sin que pueda apreciarse su relación con el contexto tecnológico, empresarial y social en el que se inscribe.

Actores principales

En cuanto a los actores principales en la construcción del discurso, ambos análisis evidencian una clara preeminencia de las voces vinculadas al negocio tecnológico.

De un lado, entre los 15 actores más influyentes en la conversación sobre big data en Twitter, 12 son medios de comunicación especializados en negocios o en tecnología, 2 son medios de comunicación generalistas, y el restante es la empresa tecnológica Intel. Por otra parte, en el caso Tay, la prensa digital adopta y reproduce de forma acrítica —en varias ocasiones repite literalmente—, el discurso oficial de Microsoft, la compañía desarrolladora del bot.

Las cuestiones más destacables sobre este contexto discursivo para el OG2 son:

9. En general, el discurso mediático adopta como propio el discurso corporativo sobre la tecnología big data, sin cuestionarlo ni aportar elementos interpretativos o discursivos para su discusión pública, más allá de aquellos que toma del mercado.

10. Reproduce una visión confusa y contradictoria de la tecnología big data, descontextualizándola del desarrollo tecnológico, el modelo de negocio y la estructura social en los que se integra.
11. Explica la relación de esta tecnología con las personas y su impacto social desde una perspectiva individualista, que favorece la atribución de responsabilidades personales y centradas en los usuarios.
12. Al infrarrepresentar determinadas explicaciones del desarrollo tecnológico y de sus efectos, no contribuye a que la ciudadanía el comprenda las posibilidades y los riesgos reales de las tecnologías big data, sino que induce a una aceptación acrítica del discurso corporativo, tomándolo como el referente natural y legitimando su opacidad.
13. Estos factores evidencian una mala praxis del periodismo en general[10]. Sorprende, dada la cantidad de estudios realizados sobre la cobertura mediática de las tecnologías emergentes que alertan sobre esta cuestión. Al mismo tiempo, dejan ver que los contextos tecnológico y corporativo antes definidos pueden estar teniendo un impacto negativo sobre la capacidad de los mismos profesionales de la comunicación para comprender y definir la situación.

[OG2–OE1+OE2+OE3] Una estructura de dominación

Antes de entrar en el cuarto apartado, parece necesario hacer dos observaciones sobre la relación general entre estos 13 primeros puntos que demuestran que, en la práctica, están fuertemente interrelacionados.

A. La lógica big data y las dinámicas de acumulación del negocio de los datos generan una creciente desigualdad de poder: las grandes tecnológicas tienen cada vez más capacidad de control sobre los datos, y la sociedad tiene cada vez menos.

B. El discurso dominante sobre la tecnología big data no fomenta la capacidad de la ciudadanía para identificar las causas estructurales de esta relación de desigualdad, ni de responder a ella de una forma organizada.

[10] En este sentido, cabe destacar que ciertas secciones de investigación de medios como *Observer* o *The New York Times* han desarrollado una tarea imprescindible al revelar los detalles de casos de corrupción de datos como los de la NSA o Cambridge Analytica.

Estos factores dan lugar a dos escenarios indeseables, que tienen una importancia central para dar respuesta al objetivo general 2 de la tesis. Esto es, para entender el impacto de las tecnologías big data en la privacidad y la libertad de las personas:

Explotación

Por una parte, los datos son tratados en este escenario general como un recurso a explotar, con el objetivo de obtener beneficios. Pero los datos no son disociables de las personas a las que se refieren. No son una propiedad de la que estas disponen y que pueden transferir. Más bien, los datos son parte de lo que una persona es y de cómo es. La explotación de los datos es, por tanto, una forma de explotar a las personas.

Dominación

Por otra parte, el contexto de desigualdad en el que se produce la explotación big data da lugar a dos formas de dominación —siguiendo la categorización de Pettit (2012)— estructural y horizontal, que se explican a continuación:

Estructural

Hay tres factores que configuran un patrón social desigual: la centralidad de los servicios digitales en las sociedades modernas; la suma de las decisiones individuales respecto a la cesión de los datos; y los discursos dominantes acerca de la situación. Estos, de forma indirecta, sitúan a las corporaciones en una posición privilegiada frente a las personas.

14. Este contexto de desigualdad representa, en sí mismo, una forma de *dominación estructural*.[11]

Horizontal

Este escenario de desigualdad, permite a las grandes corporaciones interferir más fácilmente en la vida de las personas, sin que estas puedan impedirlo.

Que dispongan de enormes cantidades de datos sobre las preferencias, los hábitos, las relaciones o las características de las personas no significa, necesariamente, que esa

[11] Véase la definición de *dominación estructural*, en la página 47.

información vaya a servir para frustrar sus intereses o manipular sus decisiones. Siendo así las cosas, esta situación no supondría un obstáculo para la libertad, si la entendemos desde su concepción liberal (*no-interferencia*).

No obstante, lo relevante aquí es que hacerlo estaría en sus manos, y que el individuo no estaría en las condiciones necesarias para ejercer una influencia en sentido contrario sobre ese proceso, es decir, no podría controlarlo. Esto es así independientemente de que la corporación quiera o no usar ese poder, de que la interferencia llegue o no a producirse, y de que la persona sea o no consciente de esa posibilidad. Lo importante es que, en cualquier caso, la corporación dispone de una capacidad de influencia que, al no ser controlable por la persona a la que afecta, deja a esta persona expuesta a su voluntad. Esto se agrava como consecuencia de la erosión de las instituciones democráticas, en la medida en que se debilitan los elementos de contención del poder de las corporaciones.

15. La relación entre las corporaciones y los usuarios representa una forma de *dominación horizontal* [12] (siguiendo la distinción de Pettit, 2012), que tiene más que ver con la *vigilancia* o, en su caso, la *intimidación*, que con la *interferencia activa*.[13]

Hay que aclarar que los términos "explotación" y "dominación" no se comprenden aquí en su sentido habitual. Tienen, por así decirlo, un sentido más político que moral. De forma más precisa: lo que pretendo no es discutir si las relaciones estudiadas son "beneficiosas" o "dañinas", sino si, independientemente de ello, contribuyen a subordinar la voluntad de unos a la de otros. El uso de los servicios de las grandes corporaciones tecnológicas puede contribuir a cubrir nuevas o viejas necesidades y hacer la vida cotidiana más cómoda, fácil o divertida. Puede, también, hacernos personas más felices. Sin negar esto, este tipo de mejoras del *bienestar* pueden no estar, actualmente, en correspondencia con un aumento de la *libertad*. Es a esto a lo que me refiero cuando hablo de la explotación y de la dominación en relación a las tecnologías big data.

[12] Véase la definición de *dominación horizontal* y *vertical* en las páginas 47 y 48.
[13] Si se dejan a un lado casos como el de Facebook-Cambridge Analytica, relacionado con un supuesto uso de los datos para manipular la decisión de los votantes, se aprecia que la interferencia activa no es la principal forma de dominación vinculada a la explotación de datos masivos.

No obstante, cabe señalar que, en la práctica, la actuación de los poderes públicos y privados en lo que respecta a la vigilancia a través de los datos no es tan lejana como podría parecer en un inicio. Además, la capacidad de la ciudadanía para intervenir en los procesos democráticos en lo que respecta al control de estas empresas, es muy reducida. Por lo tanto, y pese a que esta tesis doctoral se ha centrado en analizar la vigilancia ejercida por las grandes corporaciones (es decir, por agentes "privados"), y no tanto en la vigilancia "estatal", la forma de dominación horizontal aquí descrita no está totalmente exenta de una forma de *dominación vertical*.[14]

[OG2–OE4] La paradoja individualista

Este apartado reflexiona la reacción social ante este nuevo escenario de explotación masiva de los datos:

Una preocupación desorientada

Dos de ellas son la *paradoja de la privacidad* y la *paradoja de conocimiento*[15].

De lo que se ha visto en esta tesis, se extrae que una persona descontenta con el poder de explotación del negocio de los datos tiene dos opciones: o confiar en la buena voluntad de las grandes corporaciones, o intentar apartar su vida de la datificación. Lo segundo, como ya se ha dicho, comportaría un nivel de exigencia inasumible para la mayoría de las personas.

Existe una dificultad previa, que tiene que ver con la falta de condiciones para comprender plenamente la situación, y por lo tanto para poder valorarla como justa o injusta. Una persona común no dispone de la información suficiente para entender el uso que se está haciendo de sus datos y, si la tuviera, probablemente no podría detenerse el tiempo necesario para analizarla. En el caso de disponer de esta información, y en el supuesto de que percibiera que la situación es injusta e intentara revertirla, no lo tendría fácil para llevar a cabo sus propósitos. Hacerlo supondría adoptar una actitud radical, consistente en dejar de utilizar *todo* producto o servicio procedente de determinadas

[14] Véase la nota al pie de la página 48.
[15] Explicadas en las páginas 25 y 26.

empresas tecnológicas y sus filiales, incluidos los productos más habituales o necesarios en la vida cotidiana del ciudadano medio. La única alternativa a esto último, no siempre posible, sería disponer de conocimientos y recursos técnicos complejos para contrariar la lógica de explotación de esos productos o servicios. Y aun en el caso de aceptar que todo esto fuera viable, habría un problema adicional: esa persona no podría controlar todos los datos que otros produjesen sobre ella.

Relacionado con lo anterior, cabe señalar que la idea de privacidad predominante, como algo que "ocultar a los demás", o como un derecho a "ser dejado solo" no ayudan a comprender el tipo de impacto de la explotación big data. La dominación ejercida a través del control de los datos no es llamativa o molesta, ni tiene que ver con lo que los demás conocen de uno mismo. Lo más probable, de hecho, es que la información recogida sobre una persona no llegue a ser nunca supervisada por un humano, ni expuesta de forma pública. Esto puede generar, en aquellos que detectan que hay un riesgo derivado de la explotación de datos, una preocupación confusa y difícilmente canalizable en acciones concretas.

A esto se suma que la recopilación y el tratamiento de datos no van ligados a la introducción de un elemento claramente perjudicial para la sociedad, ni para la vida de las personas. Al contrario, hablamos de productos y servicios que también aportan grandes beneficios, como la posibilidad de mantener el contacto con amigos y familiares lejanos, disponer de información precisa sobre prácticamente cualquier cosa, o comprar productos procedentes de otra parte del mundo. Su introducción social, aunque rápida, se ha ido produciendo de forma paulatina, y el contexto social, económico y tecnológico del que forma parte no es excepcional, sino que se integra en unas dinámicas económicas y sociales mucho más amplias. Esto puede explicar, además, por qué muchas personas han aceptado que la cesión de datos es algo intrínseco a la vida moderna.

De este apartado pueden extraerse tres ideas relevantes:

16. Explicar o pretender solucionar el impacto de la explotación masiva de datos de forma individualizada es ineficaz e incoherente: por una parte, es extremadamente

complejo y sacrificado; por otra, no hace frente a la causa estructural del problema ni a su impacto social.

17. Más allá de las posibles explicaciones relacionadas con las características o atributos personales, la *paradoja de la privacidad* y la *paradoja del conocimiento* tienen mucho que ver con las formas de dominación explicadas. La paradoja de la privacidad refleja resignación, y muestra la existencia de una dificultad para canalizar la preocupación en acciones concretas o en una voz política determinada. La paradoja del conocimiento, aunque refleja una voluntad de oposición, es una buena muestra de la ineficacia de las vías de acción individual para el bien social, por muy informadas y sofisticadas que estas sean.

Una resistencia parcial

Todo lo explicado resulta también de interés para analizar dos formas de resistencia propuestas por personas y grupos particularmente sensibilizados con las amenazas de la explotación big data: el *suicidio digital* y la *ofuscación*.[16]

Por una parte, dejar de utilizar todos los productos o servicios de determinadas empresas, como por ejemplo Google, es especialmente complicado. Para ello, uno tendría que dejar de utilizar su buscador, su navegador, sus distintos sistemas operativos, su servicio de correo electrónico, su servidor de mapas interactivos, sus herramientas de cálculo o de elaboración de formularios, sus aplicaciones de mensajería o sus sistemas de almacenamiento de información. Son sólo algunos ejemplos. Implicaría dejar de utilizar, además, cualquier otro producto o servicio dependiente de los anteriores, o interactuar con personas que utilicen estos servicios (enviar un email a una persona con Gmail da información a Google sobre esta interacción). El suicidio digital, además de exagerado, es ineficaz: mientras se reduzca a la acción aislada de algunas personas, no supone ninguna forma de influencia sobre el poder las grandes corporaciones tecnológicas. Consiste únicamente en una forma de autocensura que, incluso en su forma más exitosa a nivel individual, no contrarresta los efectos de la dominación.

[16] Explicadas en las páginas 26 y 27.

Por otra parte, las técnicas de ofuscación, que operan en herramientas como TrackMeNot o AdNauseam, consisten en generar cantidades enormes de datos, impidiendo así dibujar el perfil real de la persona que las utiliza. Este enfoque parece la forma más efectiva de oponerse individualmente a la explotación de datos masivos, en tanto que desafía su lógica técnica: se sirve de ella para contrarrestarla. Sin embargo, de nuevo, es una alternativa que no trasciende el nivel individual y que, además, es difícilmente extensible a individuos o círculos sociales que desconocen la situación, que no tienen una preocupación clara y definida por el problema, que no comprenden su parte técnica, o que no ven la necesidad de actuar contra él. Por otra parte, estas herramientas no son aplicables a todos los productos o servicios de las diferentes compañías implicadas en la explotación de datos, ni a todas las formas de relación de un usuario con dichos productos. Más que ser una solución al problema, es un efectivo parche contra algunos de sus efectos.

Las cuestiones a destacar de este apartado son las siguientes:

18. El suicidio digital y la ofuscación son respuestas individuales, pensadas para personas altamente concienciadas y con un conocimiento técnico del problema, que están dispuestas para actuar frente a la situación.
19. Son dos respuestas que no permiten salir de forma plena del ámbito de influencia de los grandes explotadores de datos.
20. Se trata de herramientas que, en la medida en que no son extensibles al conjunto de la ciudadanía, no constituyen una verdadera solución al problema de dominación.

[OG2–OE5] Ineficacia política del RGPD

Teniendo en cuenta la naturaleza problema generado por la explotación big data que se ha definido hasta el momento, esta sección reflexiona sobre la capacidad del modelo europeo de protección de datos, establecido en el RGPD, para hacerle frente de forma eficaz. Es importante destacar que esta tesis doctoral no se ha centrado en las carencias de aplicación actual de los mecanismos establecidos por el marco jurídico europeo, sino en valorar si, en el caso de su correcta aplicación, sería efectivo.

El RGPD tiene dos objetivos:

- El primero es dar cumplimiento al derecho fundamental de las personas "a la protección de los datos de carácter personal que le conciernan, en lo que respecta al tratamiento de esos datos". Este objetivo se plantea como solución al reciente desarrollo tecnológico y a la creciente preocupación ciudadana por su privacidad, especialmente ante los casos de "violación" de datos.
- El segundo es promover la libre circulación de tales datos. Este responde a la pérdida (o el no-aumento) de beneficios de las empresas europeas derivada de la desconfianza ciudadana en aquellas que operan en el entorno digital [17].

Existe una cierta tensión entre ambos objetivos. Por un lado, los datos se conciben como un bien con un importante valor económico. En concreto, los beneficios relacionados con la explotación de datos se estiman en "206.000 millones de euros" entre 2016 y 2020 (Enero de 2016b). Por otro lado, el reglamento se presenta como garante del derecho fundamental a la protección de los datos personales, reconocido en el artículo 8 de la Carta de la Unión Europea. Aunque el grado de tensión entre ambas cuestiones dependerá de la concepción que se tenga de los derechos fundamentales, algo en lo que no entraremos aquí, lo que sí parece claro es que el reglamento no es lo suficientemente claro en sus propósitos: el fomento del negocio de los datos, entendidos como bienes económicos, podría dañar el derecho fundamental que toda persona tiene a la protección de los mismos.

El consentimiento individual

El RGPD sigue el modelo de la notificación y el consentimiento. No obstante, el consentimiento, en tanto que elemento principal de la protección, plantea serios problemas para proteger a las personas del impacto de la explotación big data:

Debido a la dificultad de informar específicamente sobre los procesos de recopilación y tratamiento de los datos, y al esfuerzo que supondría para los usuarios estar al corriente de los mismos, generalmente el consentimiento se proporciona de forma previa, como un preacuerdo para poder utilizar un determinado producto o servicio. Si, como está establecido, el consentimiento se proporciona de forma previa a la recopilación y al

[17] Esto se refiere a la explicación que se aporta en la página 29.

tratamiento de los datos, es un mecanismo que no permite tomar una decisión relevante, porque se otorga sin poder tener en cuenta la información que se obtendrá de los datos tras su tratamiento.

- El consentimiento individual previo al tratamiento de los datos no es válido ni significativo.

El consentimiento representa una forma de autoprotección que, como ya se ha explicado, no puede hacer frente a una amenaza estructural. Además, dada la imposibilidad objetiva de los ciudadanos para controlar el poder de influencia de las grandes empresas tecnológicas, este se convierte, más bien, en una forma de legitimar la dominación: el individuo consiente un poder de interferencia, sobre el que no tiene control.

- El consentimiento individual no representa una decisión libre.

Estos problemas se derivan, como se ha ido explicando a lo largo de esta tesis, de la concepción liberal de la privacidad (como una esfera inviolable) y de la libertad (como no-interferencia) que están en la base del reglamento. De acuerdo con esta lógica, proteger a las personas de los efectos del tratamiento de sus datos consiste en lo siguiente: partiendo de que la relación entre la parte interesada en el tratamiento de los datos y la persona a la que "conciernen" estos datos es "privada", dicha persona debe poder decidir si cede o no sus datos, sin que su decisión sea injustificadamente impuesta por la otra parte. Es decir, se trata de evitar que la persona sea "víctima" de una "violación de sus datos", o que sea obligada a ceder más datos de los que se requieren para un fin determinado. Sin embargo, esta tesis ha argumentado que el principal problema de la explotación de datos masivos no tiene que ver con esta amenaza de interferencia individualizada y directa.

A continuación, se introduce una última observación general, acerca de si es pertinente que el Reglamento se ocupe, únicamente, de los datos "personales".

Datos personales, *perfilantes* y sociales

A fin de entender mejor qué tipo de protección es necesaria ante el impacto de la explotación de datos masivos, se podrían identificar tres tipos de datos "personales": los

datos personales propiamente dichos, los *perfilantes* y los *sociales*. Para no complicar la argumentación, se acepta la definición de "datos personales" dada por el RGPD, y se añaden después dos definiciones adicionales:

- Datos personales: toda información vinculada a un *identificador*[18] que determina o permite determinar la identidad de la persona física a la cual concierne esta información.
- Dentro de los datos personales, existe una categoría "especial" de datos "particularmente sensibles"[19].
- Datos *perfilantes*[20]: toda información que concierne a una persona física, cuya identidad no es identificable, o no es plenamente identificable.
- Datos sociales: toda información que se refiere exclusivamente a un conjunto de personas, no identificadas individualmente.

Lo que tienen en común estas tres categorías es que definen tipos de datos relativos a preferencias, comportamientos, conductas, hábitos o características de *personas*, ya sea a nivel individual o colectivo, e independientemente de que se pueda determinar de forma indiscutible la identidad concreta de la persona a la que se refieren. No son objeto de esta clasificación, por lo tanto, los datos referidos al mundo físico o natural, como por ejemplo datos sobre el suelo, el clima, o una determinada especie vegetal o animal, etc. La explotación de los datos de los que estamos hablando, ya sean personales, *perfilantes* o sociales, puede tener un impacto directo o indirecto sobre la vida o las decisiones de las personas a las que se refieren. El Reglamento, al ocuparse solamente de los datos personales, no responde adecuadamente a las diferentes clases de impacto que puede tener la explotación de los otros dos tipos de datos.

A estos problemas del RGPD, se suman otros que no tienen que ver únicamente con la esfera jurídica, sino más generalmente con el papel de las instituciones públicas, tanto nacionales como europeas. Como ya se ha señalado en apartados anteriores, el modelo

[18] Véase la definición aportada en la página 30.
[19] Veáse la definición de datos sensibles en la página 31.
[20] El neologismo '*perfilantes*' se entiende aquí como derivación del sustantivo 'perfil'. Las tres primeras acepciones de "perfil" en el diccionario de la Real Academia Española (RAE) son: "1. m. Postura en que no se deja ver sino una sola de las dos mitades laterales del cuerpo. 2. m. Contorno de la figura de algo o de alguien. 3. m. Conjunto de rasgos peculiares que caracterizan a alguien o algo."

jurídico de protección de datos no viene acompañado de acciones políticas capaces de hacer frente a la creciente concentración de poder de las grandes empresas tecnológicas.

En definitiva, y para concluir la lista de aportaciones describe el impacto de cada uno de los cinco contextos analizados:

21. El modelo establecido por el RGPD protege a las personas de los casos de interferencia activa más flagrantes, como aquellos relacionados con el robo de datos o de uso ilícito o desproporcionado de los mismos. Sin embargo olvida u omite muchos otros problemas, igualmente nocivos para la privacidad y la libertad.
22. El modelo de protección no responde adecuadamente a uno de los objetivos que el propio reglamento se marca: actuar sobre las causas de la preocupación de la ciudadanía europea respecto a su privacidad, garantizando el derecho fundamental de todas las personas a la protección de sus datos.
23. Al plantearse la protección de los datos como una cuestión personal, basada en la responsabilidad individual, el objetivo de protección social al que pretende dar respuesta el RGPD queda soslayado, o es cumplido solamente de forma parcial.
24. El RGPD es incoherente con el contexto de la explotación de datos y propone un mecanismo inadecuado para responder los problemas que genera ese contexto. Esto quiere decir que, aunque el RGPD cumpliese los objetivos que se plantea (evitar interferencias), no sería eficaz para hacer frente a la complejidad del problema que ha identificado esta tesis.
25. Por último, parece necesario repensar los mecanismos de protección de las personas frente a la vigilancia masiva desde la perspectiva de las teorías feminista y republicana.

Conclusiones

Durante las dos últimas décadas, el desarrollo de internet y de los medios sociales han cambiado la forma de comunicarse, de relacionarse, de informarse y de consumir. Esto ha provocado una creciente digitalización de la vida cotidiana que genera un escenario insólito: cada vez más características, preferencias y comportamientos de las personas se registran en forma de datos. En paralelo, se han desarrollado las tecnologías necesarias para recopilar y procesar todos esos datos de forma rápida, sofisticada y, necesariamente, automatizada.

A raíz del gran escándalo de corrupción de datos revelado por Snowden en 2013, el fenómeno big data ha despertado un gran interés a todos los niveles de la sociedad. Los medios de comunicación hablan recurrentemente de las tecnologías big data, los estudios y encuestas revelan que la ciudanía las percibe con preocupación, y la academia investiga sus oportunidades y sus riesgos. Mientras tanto, se ha ido consolidando un nuevo modelo de negocio basado en la explotación masiva de datos, que ha convertido a las grandes corporaciones tecnológicas proveedoras de servicios digitales en unas de las más pujantes a escala global. Fundamentalmente, Google, Amazon, Facebook, Apple y Microsoft. En Europa, estos cambios han propiciado la reciente entrada en vigor de un nuevo Reglamento General de Protección de Datos.

Esta tesis por compendio de publicaciones ha presentado una revisión actualizada de la investigación contemporánea sobre el fenómeno big data. Además, ha definido las características principales de cinco contextos que determinan la estructura general en la que se integra la explotación de datos masivos: 1. la lógica de generación, recopilación y procesamiento de datos masivos; 2. el modelo de negocio de las grandes corporaciones tecnológicas de servicios digitales y su encaje en el sistema económico capitalista; 3. el discurso mediático predominante sobre las tecnologías big data; 4. las reacciones sociales mayoritarias y las formas de resistencia a la explotación propuestas por los sectores especializados; y 5. el modelo jurídico europeo de protección de datos. La investigación se ha centrado en examinar estos factores a la luz de una perspectiva teórica original, fundamentada en la teoría de framing, la crítica feminista a la privacidad, los estudios críticos sobre el capitalismo y la filosofía neorrepublicana.

Mediante este estudio se han identificado diferentes obstáculos que limitan la capacidad de la ciudadanía europea para ejercer sus derechos fundamentales a la privacidad y a la protección de datos. En su conjunto, la tesis explica cuál es el tipo de impacto social y político de las tecnologías big data. Al mismo tiempo, señala una alternativa desde la cual repensar el papel social de las tecnologías big data, los objetivos de la acción individual y política, y las dinámicas del mercado, los medios de comunicación y de la propia academia respecto al uso de datos masivos.

Los siguientes diez puntos resumen las conclusiones principales de la memoria y las cinco publicaciones de la tesis:

1. La lógica de generación, recopilación y procesamiento de datos masivos hace imposible dejar de difundir datos y mantener la propia vida al margen de la datificación. A medida que estas técnicas se desarrollan, se vuelven también más opacas, imprevisibles e incontrolables. De este modo, se reducen las posibilidades de controlar los datos y proteger su privacidad.

2. Esta tendencia al descontrol es particularmente beneficiosa para el modelo de negocio de los gigantes digitales. Es, también, indisociable de tres dinámicas propias del entorno de internet que contribuyen a que estas grandes corporaciones tecnológicas monopolicen el mercado de los servicios digitales: los efectos de red, la publicidad basada en datos como fuente de ingresos y la importancia de los estándares técnicos.

3. El valor económico que han adquirido los datos que recopilan estas multinacionales les ha otorgado un gran peso en la economía global. Esto, sumado al potencial de estos datos para el control social, les permite ejercer fuertes presiones sobre los poderes públicos para que implementen políticas impositivas y regulaciones favorables a sus intereses comerciales. Esto genera un desgaste paulatino de la capacidad de las instituciones democráticas para hacer frente a su poder.

4. Los dos análisis empíricos realizados muestran que la representación mediática mayoritaria de las tecnologías big data es sesgada, descontextualizada y reproduce el discurso corporativo sin apenas introducir elementos discursivos e interpretativos nuevos. Esto limita la voz política de la ciudadanía e induce a una actitud acrítica y a una comprensión individualista de los efectos de su introducción social y de las posibles

reacciones frente a ellos. No obstante, cabe tener en cuenta que esta mala praxis puede estar reflejando, también, las consecuencias de la opacidad tecnológica.

5. Estos cuatro primeros elementos generan un patrón social que sitúa a las grandes corporaciones en una posición de privilegio con respecto a la ciudadanía. Esto representa una forma de *dominación estructural* que vicia la capacidad (reduce la libertad de oportunidad) de la ciudadanía para decidir libremente sobre sus datos.

6. Bajo esta desigualdad de condiciones, los gigantes digitales disponen de un poder de interferencia en la vida de las personas, que estas carecen de recursos materiales e inmateriales para controlar. Esta relación de *dominación* (*horizontal*, según la categorización de Pettit, 2012), representa una invasión de la voluntad (reduce la libertad de control) de la ciudadanía de ejercer sus derechos a la privacidad y la protección de los datos. Es una forma de control que tiene más que ver con la vigilancia o, en su caso, la intimidación, que con la interferencia directa y deliberada en las decisiones personales. Esto no quiere decir que esta relación produzca malestar o infelicidad en las personas que la sufren, sino que, independientemente de ello, contribuye a subordinar su voluntad a los intereses de estas empresas.

7. Este escenario de dominación permite comprender que, ciertas respuestas contradictorias, como la paradoja de la privacidad, pueden no deberse única y exclusivamente a características o circunstancias personales. Más bien, la explicación parece relacionada con la falta de las condiciones objetivas y cognitivas necesarias para actuar de forma coherente a las propias preocupaciones.

8. Los sectores sociales más informados y críticos con la situación proponen el suicidio digital y la ofuscación como dos formas de resistencia frente a la explotación big data. Ambas son iniciativas útiles e interesantes, pero no representan una solución al escenario de dominación, en tanto que no afectan a todos los ámbitos en los que se produce la explotación, no permiten controlar el poder de interferencia de las grandes corporaciones, ni son una opción extensible al conjunto de la ciudadanía.

9. Frente a esta situación, el nuevo Reglamento General de Protección de Datos de la Unión Europea se fundamenta en una concepción liberal de la libertad y de la privacidad, fundamentalmente preocupada por los casos de violación de los datos. Esta

perspectiva da lugar a un modelo de protección basado en el consentimiento individual, que es incoherente con la lógica de las tecnologías big data, e incapaz de hacer frente a la desigualdad de poder en la que estas se desarrollan y se utilizan.

10. Atendiendo a estos factores, parece más adecuado y eficaz repensar la respuesta social a los abusos de la explotación big data (incluyendo el modelo de protección de datos) desde una concepción republicana de la privacidad y de la libertad como *no-dominación*. Esto no supone renunciar al gran potencial de las tecnologías big data, ni reemplazar la decisión "privada" como mecanismo principal de protección de los datos, u obligar a las personas a mantener sus datos en secreto. Al contrario, tiene que ver con asegurar las condiciones (objetivas y cognitivas, materiales e inmateriales) necesarias para que esta decisión responda, verdaderamente, a la voluntad de las personas y les permita ejercer control sobre los procesos a los que se someten los datos. Para garantizar esta cuestión, el desarrollo de las tecnologías big data debe ser más transparente, responsable, controlable, y atender a intereses compartidos, y no privados. Esto significa, también, limitar la excesiva concentración de poder de las grandes multinacionales tecnológicas. En este sentido, la acción no puede ser únicamente individual, sino que debe ser democráticamente decidida y capaz de hacer frente a su extensión internacional.

En definitiva, una protección más efectiva de las personas frente al impacto de la explotación big data sería una basada en la redistribución de recursos, más preocupada por que la ciudadanía pueda controlar a los diferentes poderes interesados en la explotación de sus datos, y más centrada en la justicia social que en la reacción individual.

Limitaciones e investigaciones futuras

Esta tesis doctoral ha explorado el impacto de la explotación de datos masivos desde una perspectiva amplia. Quizás en parte debido a ello, se ha encontrado con algunas dificultades, y tiene ciertas limitaciones, a las que este capítulo pretende dar respuesta.

Una primera cuestión, que puede dificultar la comprensión de la tesis, es que algunos de los conceptos centrales que en ella se trabajan, como "big data", "privacidad", "libertad" o, incluso, "datos personales", son especialmente confusos y están en permanente disputa. Esto podría dar lugar a interpretaciones diversas, o contradictorias, dependiendo de la concepción que tenga de ellos el lector. Con todo, esta dificultad se ha señalado a lo largo de la tesis, y se ha intentado subsanar utilizando los términos de una forma coherente y argumentada.

Por otra parte, esta investigación no se ha ocupado en profundidad de la dicotomía público-privado y, por el contrario, ha prestado mucha atención a las diferentes ideas de *libertad*. Esta elección podría parecer poco adecuada, dado que el problema de la explotación big data suele abordarse en los términos de esta dicotomía. No obstante, y pese a que la privacidad es un concepto relevante en la tesis, esto tiene una explicación que me gustaría subrayar aquí. Una de las aportaciones de la tesis es mostrar que la privacidad es una esfera cuyo significado y cuya protección varían en función de cómo uno entienda la libertad. En consecuencia, la reflexión se ha centrado en señalar los problemas de la idea liberal de libertad (*no-interferencia*), que subyace a la concepción hegemónica de la privacidad. La conclusión de este análisis ha sido que la concepción republicana de libertad daría un sentido y un alcance distintos a la privacidad, ligado a la *insubordinabilidad* de las decisiones que afectan a la protección de los datos personales. El motivo es que los problemas de la explotación de datos para la privacidad de las personas se inscriben en un contexto más amplio de *dominación*.

Otra de las limitaciones de la tesis tiene que ver con el planteamiento metodológico de los dos estudios empíricos. Ambos parten de una muestra limitada, aunque suficiente, para establecer una primera aproximación al tema. No obstante, los resultados extraídos, analizados a la luz de otras investigaciones previas sobre la representación mediática de la tecnología emergente, en general, y de la tecnología big data, en particular, han

permitido extraer conclusiones interesantes para el cumplimiento de los objetivos generales planteados.

En tercer lugar, cabe destacar que, dada la misma naturaleza del problema estudiado, esta investigación se ha visto en la necesidad de tener en cuenta las aportaciones de disciplinas diversas. La mayoría de ellas proceden del ámbito de la Comunicación y las Ciencias de la Información o, más generalmente de las Ciencias Sociales. Pero hay otras que entran más bien en los terrenos de la Teoría o la Filosofía Política y de la Informática o la Computación. Este es un obstáculo que, para dar cuenta del contexto general de la explotación big data, era necesario afrontar. En el caso concreto del examen del Reglamento europeo, en el que la distancia con respecto a mi bagaje podría parecer más problemática, es importante destacar que la pretensión no ha sido realizar un análisis técnico, o profundizar en cuestiones de interpretación de la norma, sino únicamente entender cuál es sentido general de la ley, desde un punto de vista teórico o conceptual. Lo mismo ocurre en relación a los aspectos más técnicos del procesamiento de datos masivos o el aprendizaje de máquinas. Aquí, el inconveniente se ha solventado mediante lecturas especializadas, reforzadas por la explicación de otros autores del ámbito de las Ciencias Sociales, o por grupos interdisciplinares.

En ambos casos, antes de ser definitivamente plasmados en esta memoria, los resultados de la investigación han sido presentados en varias actividades del Programa de Doctorado en Comunicación, así como en congresos y seminarios internacionales ante audiencias de los diferentes ámbitos que abarca la tesis. Además, se han consultado con profesores especializados en áreas distintas a la propia.

Soy consciente, también, de que la tesis se ha enfocado desde una perspectiva más crítica que propositiva. Este enfoque tiene la ventaja de que me ha permitido alcanzar un conocimiento profundo de la situación que rodea a las tecnologías big data. Espero que esta base sea el punto de partida de investigaciones futuras, más propositivas. En concreto, la concepción de libertad como *no-dominación* y las teorías republicanas de justicia social y de legitimidad política, que se han introducido aquí como un elemento de análisis crítico, pueden ser útiles no solo para seguir profundizando en la explicación del problema, sino también para plantear posibles soluciones.

Bibliografía

AdNauseam. Clicking ads so you don't have to (2019) [Página web]. Disponible en: https://adnauseam.io/.

Agra Romero, María Xosé (2012). El feminismo y/en la filosofía política, *Laguna. Revista de Filosofía, 30*: 31-46. Disponible en: http://riull.ull.es/xmlui/handle/915/2450.

AI Now Institute (2019) [Página web]. Disponible en: https://ainowinstitute.org/.

Allen, Anita L. (1999). Coercing Privacy, *Faculty Scholarship. Paper 803. William and Mary Law Review, 40*(3): 723-757. Disponible en: https://scholarship.law.upenn.edu/faculty_scholarship/803.

Allen, Anita L. (2006). Protecting One's Own Privacy in a Big Data Economy, *University of Pennsylvania Law School, Public Law and Legal Theory Research Paper Series. Research Paper No. 17-1, Harvard Law Review Forum, 130*: 71-78. Disponible en: http://ssrn.com/abstract=2894545.

Allen, Anita, L. (2011). *Unpopular Privacy: What Must We Hide?* Nueva York: Oxford University Press.

Antunes, Deborah Cristina y Maia, Ari Fernando (2018). Big Data, ubiquitous exploitation, and targeted advertising: New facets of the cultural industry, *Psicología USP, 29*(2): 189-199. doi: 10.1590/0103-656420170156.

Arruzza, Cinzia; Bhattacharya, Tithi y Fraser, Nancy (2019). *Feminism for the 99%. A manifesto*. Londres, Brooklyn: Verso, New Left Books.

Barnes, Susan B. (2006). A privacy paradox: Social networking in the United States, *First Monday, 11*(9): 1-10. doi: https://doi.org/10.5210/fm.v11i9.1394.

Bartlett, Jamie (2018). *The People Vs Tech. How the internet is killing democracy (and how we save it)*. Nueva York: Dutton-Penguin Random House.

Baruh, Lemi y Popescu, Mihaela (2017). Big data analytics and the limits of privacy self-management, *New media & Society, 19*(4): 579-596. doi: https://doi.org/10.1177/1461444815614001.

Bellamy, Richard (2019). *A Republican Europe of States. Cosmopolitanism, Intergovernmentalism and Democracy in the EU*. Cambridge: Cambridge University Press.

Berlin, Isaiah (1969). *Four Essays On Liberty*. Oxford, England: Oxford University Press.

Bobbio, Norberto (2009). *Igualdad y libertad*. Barcelona: Paidós Ibérica.

Bogomolov, Andrey; Lepri, Bruno; Staiano, Jacopo; Oliver, Nuria; Pianesi, Fabio y Pentland, Alex (Sandy) (2014). Once upon a crime: Towards crime prediction from demographics and mobile data, *Proceedingss of the 16th International Conference on Multimodal Interaction*: 427-434. doi: http://dx.doi.org/10.1145/2663204.2663254.

Bohman, James (2007). *Democracy across Borders: from Dêmos to Dêmoi*. Cambridge, Londres: The MIT Press.

boyd, danah y Crawford, Kate (2011). Six Provocations for Big Data, *Paper presented at: A decade in internet time: Symposium on the dynamics of the internet and society,* Oxford Internet Institute. doi: http://dx.doi.org/10.2139/ssrn.1926431.

boyd, danah, Levy, Karen y Marwick, Alice. 'The networked nature of algorithmic discrimination'. En Peña Gangadharan, Seeta (ed.) (2014) *Data and discrimination: Collected essays*. Distrito de Columbia (Washington): Open Technology Institute - New America Foundation.

Brunton, Finn y Nissembaum, Helen (2015). *Obfuscation: A User's Guide for Privacy and Protest*. Londres: The MIT Press.

Burkell, Jacquelyn; Fortier, Alexandre; Yeung Cheryl Wong, Lorraine (Lola) y Simpson, Jennifer-Lynn (2014). Facebook: Public space, or private space?, *Information, Communication & Society, 17*(8): 974-985. doi: https://doi.org/10.1080/1369118X.2013.870591.

Cadwalladr, Carole (17 de marzo de 2018). I made Steve Bannon's psychological warfare tool': meet the data war whistleblower, *Observer - The Guardian*. Disponible

en: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

Cadwalladr, Carole (7 de mayo de 2017). The great British Brexit robbery: how our democracy was hijacked, *Observer - The Guardian*. Disponible en: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

Cadwalladr, Carole y Graham-Harrison, Emma (17 de marzo de 2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, *Observer - The Guardian*. Disponible en: https://www.theguardian.com/news/2018/mar/17/cambridgeanalytica-facebook-influence-us-election.

Caplan, Rob y boyd, danah (2016). Who controls the public sphere in an era of algorithms? Mediation, automation, power, *Contemporary Issues and Concerns Primer, Data & Society Research Institute*. Disponible en: https://datasociety.net/events/who-controls-public-sphere.

Carta de Derechos Fundamentales de la Unión Europea (2016/C 202/2). Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=uriserv:OJ.C_.2016.202.01.0389.01.SPA.

Castells, Manuel (2009). *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. Cambridge: Blackwell Publishers.

Castillo, Carlos (2016). *Big crisis data. Social Media in Disasters and Time-Critical Situations.* Cambridge University Press.

Centre Internet et Société (2019) [Página web]. Disponible en: http://cis.cnrs.fr/.

Centro de Investigaciones Sociológicas (CIS) (febrero de 2017). *Barómetro de febrero 2017. Estudio nº3168*. Disponible en: http://www.cis.es/cis/export/sites/default/-Archivos/Marginales/3160_3179/3168/es3168mar.pdf.

Chandler, David y Fuchs, Christian (eds.) (2019). *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*. Londres: University of Westminster Press.

Cohen, Julie (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven, Londres: Yale University Press.

Cohen, Julie [*pendiente de publicación en octubre de 2019*]. *Between Truth and Power: The Legal Construction of Informational Capitalism*. Oxford: Oxford University Press.

Cox, Michael y Ellsworth, David (1997). *Application controlled demand paging for out-of-core visualization. Report NAS-97-010, July 1997.* Moffet Field: NASA Ames Research Centre. Disponible en: https://www.nas.nasa.gov/assets/pdf/techreports/1997/nas-97-010.pdf.

Data & Society Research Institute (2019) [Página web]. Disponible en: https://datasociety.net/.

Data activism: The politics of big data according to civil society. DATACTIVE Research project (2019) [Página web]. Disponible en: https://data-activism.net/about/.

Data Justice Lab (2019) [Página web]. Disponible en: https://datajusticelab.org/.

Data Justice: Understanding datafication in relation to social justice. DATAJUSTICE Research Project (2019) [Página web]. Disponible en: https://datajusticeproject.net/.

Dirección General de Justicia y Consumidores de la Comisión Europea (2016) (última actualización en enero de 2017). *Data Protection Reform. Factsheets*. Disponible en: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. [Directiva derogada]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A31995L0046.

Dockray, Sean (31 de mayo de 2010). The Facebook suicide bomb manifesto, *Wired [antes publicado en la lista de distribución de correo electrónico del iDC - Institute for*

Distributed Creativity]. Disponible en: https://www.wired.com/2010/05/the-facebook-suicide-bomb-manifesto/.

Druckman, James, N. y Bolsen, Toby (2011). Framing, Motivated Reasoning, and Opinions About Emergent Technologies, *Journal of Communication, 61*(4): 659-688. doi: 10.1111/j.1460-2466.2011.01562.x.

Dulong de Rosnay, Mélanie (2016). *Les Golems du numérique. Droit d'auteur et Lex Electronica*. París: Presses des Mines.

Entman, Robert M. (1993). Framing: Toward Clarification of a Fractured Paradigm, *Journal of Communication, 43*(4): 51-58. doi: https://doi.org/10.1111/j.1460-2466.1993.tb01304.x.

Eticas Foundation (2019) [Página web]. Disponible en: https://eticasfoundation.org/.

Etzioni, Amitai (1999). *The Limits of Privacy*. Nueva York: Basic Books.

Facebook for business (8 de mayo de 2014). *Learn more about the people that matter to your business with Facebook audience insights* [Comunicado oficial]. Disponible en: https://www.facebook.com/business/news/audience-insights.

Federici, Silvia (2004). *Caliban and the witch. Women, the body and primitive accumulation*. Brooklyn: Autonomedia.

Federici, Silvia y Taylor, Astra (Junio de 2019). Silvia Federici in Conversation with Astra Taylor, *The Believer*. Disponible en: https://believermag.com/silvia-federici-in-conversation-with-astra-taylor/.

Feenstra, Ramón (2018). Kidnapped democracy: how can citizens escape? *The Conversation - Revolutions and Counter Revolutions series.* Disponible en: http://theconversation.com/kidnapped-democracy-how-can-citizens-escape-90011.

Feenstra, Ramón [*pendiente de publicación en noviembre de 2019*]. *Kidnapped Democracy*. Londres: Rowman & Littlefield International.

Fernández-Manzano, Eva-Patricia; Neira, Elena y Clares-Gavilán, Judith (2016). Data management in audiovisual business: Netflix as a case study, *El profesional de la información, 25*(4): 568-576. doi: http://dx.doi.org/10.3145/epi.2016.jul.06.

Floridi, Luciano (2011). *The Philosophy of Information*. Oxford: Oxford University Press.

Floridi, Luciano (2013). *The Ethics of Information*. Oxford: Oxford University Press.

Floridi, Luciano (2019). *The Logic of Information*. Oxford: Oxford University Press.

Fraser, Nancy (2012). On Justice. Lessons from Plato, Rawls and Ishiguro. *New Left Review 74*(March-April 2012): 41-51. Disponible en: https://newleftreview.org/II/74/nancy-fraser-on-justice.

Fraser, Nancy (2017). Progressive Neoliberalism versus Reactionary Populism: A Choice that Feminists Should Refuse, *NORA - Nordic Journal of Feminist and Gender Research, 24(*4): 281-284. doi: https://doi.org/10.1080/08038740.2016.1278263.

Galdón Clavell, Gemma (2018). Exploring the ethical, organisational and technological challenges of crime mapping: a critical approach to urban safety technologies, *Ethics and Information Technology, 20*(4): 265-277. doi: https://doi.org/10.1007/s10676-018-9477-1.

Gellman, Barton y Poitras, Laura (7 de junio de 2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, *The Washington Post*. Disponible en: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.df0206d7bfe6.

Goffman, Erving (1975). *Frame Analysis: An Essay on the Organization of Experience*. Cambridge: Harvard University Press.

Gräf, Eike (2017). When Automated Profiling Threatens Our Freedom: A Neo-Republican Perspective, *European Data Protection Law Review, 3*(4): 441-451. doi: https://doi.org/10.21552/edpl/2017/4/6.

Greenwald, Glenn; MacAskill, Ewen y Poitras, Laura (11 de junio de 2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations, *The Guardian*. Disponible en: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Guerrero-Solé, Frederic (2017). Community Detection in Political Discussions on Twitter: An Application of the Retweet Overlap Network Method to the Catalan Process Toward Independence, *Social Science Computer Review, 35*(2): 244-261. doi: https://doi.org/10.1177/0894439315617254.

Guerrero-Solé, Frederic (2018). Interactive Behavior in Political Discussions on Twitter: Politicians, Media, and Citizens' Patterns of Interaction in the 2015 and 2016 Electoral Campaigns in Spain, *Social Media + Society, 4*(4): 1-16. doi: https://doi.org/10.1177/2056305118808776.

Guerrero-Solé, Frederic; Corominas-Murtra, Bernat y Lopez-Gonzalez, Hibai (2014). Pacts with Twitter. Predicting voters' indecision and preferences for coalitions in multiparty systems, *Information, Communication & Society, 17*(10): 1280-1297. doi: https://doi.org/10.1080/1369118X.2014.920040.

Guerrero-Solé, Frederic y Lopez-Gonzalez, Hibai (2019). Government Formation and Political Discussions in Twitter: An Extended Model for Quantifying Political Distances in Multiparty Democracies, *Social Science Computer Review, 37*(1): 3-21. doi: https://doi.org/10.1177/0894439317744163.

Halavais, Alexander (2015). Bigger sociological imaginations Framing big social data theory and methods, *Information, Communication & Society, 18*(5): 583-594. doi: https://doi.org/10.1080/1369118X.2015.1008543

Hallinan, Blake y Striphas, Ted (2016). Recommended for you: The Netflix Prize and the production of algorithmic culture. *New Media and Society, 18*(1), 117-137. doi: https://doi.org/10.1177/1461444814538646.

Hanisch, Carol (1970). The personal is political, *Notes From the Second Year: Women's Liberation. Major Writings of the Radical Feminists*: 76-78.

Hanisch, Carol (2006). The personal is political. The Women's Liberation Movement classic with a new explanatory introduction. *Women of the World, Unite! Writings by Carol Hanisch* [Página web]. Disponible en: http://www.carolhanisch.org/CHwritings/PIP.html.

Hargittai, Eszter y Marwick, Alice (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy, *International Journal of Communication, 10*(2016): 3737-3757. Disponible en: https://ijoc.org/index.php/ijoc/article/view/4655/1738.

Harvey, David (2005). *A brief history of Neoliberalism*. Nueva York: Oxford University Press.

Herman, Edward S. y Chomsky, Noam (2002). *Manufacturing Consent. The Political Economy of the Mass Media*. Nueva York: Pantheon Books.

Hintz, Arne; Dencik, Lina y Wahl-Jorgensen, Karin (2019). *Digital citizenship in a datafied society*. Cambridge: Polity Press.

Hobbes, Thomas (2011) [1651]. *Leviatán, o la materia, forma y poder de un Estado eclesiástico y civil.* Madrid: Alianza Editorial.

Howe, Daniel C. y Nissenbaum, Helen (2017). Engineering privacy and protest: A case study of AdNauseam, *CEUR Workshop Proceedings, 1873*: 57-64. Disponible en: http://ceur-ws.org/Vol-1873/IWPE17_paper_23.pdf.

Howe, Daniel C. y Nissenbaum, Helen. 'TrackMeNot: Resisting Surveillance in Web Search'. En: Kerr, Ian; Lucock, Carole y Steeves, Valerie (eds.) (2009). *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press.

Hoye, J. Matthew y Monaghan, Jeffrey (2015). Surveillance, freedom and the republic, *European Journal of Political Theory, 17*(3): 343-363. doi: https://doi.org/10.1177/1474885115608783.

Ishiguro, Kazuo (10 de septiembre de 2010). *Kazuo Ishiguro discusses his intention behind writing the novel, Never Let Me Go* [entrevista en formato video en YouTube], Film Independent. Disponible en: https://www.youtube.com/watch?v=_jCB59pPG7k.

Ishiguro, Kazuo (2005). *Never Let Me Go*. Londres: Faber and Faber, 2006.

Jourová, Vêra (Enero de 2016a). Ficha Informativa. ¿Cómo refuerza la reforma de la protección de datos los derechos de los ciudadanos? *Dirección General de Justicia y Consumidores: Data Protection Reform.* Disponible en: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41596.

Jourová, Vêra (Enero de 2016b). Ficha Informativa. La reforma de la protección de datos en la UE y los macrodatos. *Dirección General de Justicia y Consumidores: Data Protection Reform.* Disponible en: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41594.

Jourová, Vêra (Enero de 2016c). Ficha Informativa. ¿Cómo afectará la reforma de la protección de datos a las redes sociales? *Dirección General de Justicia y Consumidores: Data Protection Reform.* Disponible en: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41590.

Jourová, Vêra (Enero de 2016d). Ficha Informativa. ¿De qué modo adaptará la reforma de la protección de datos en la UE la normativa vigente a la evolución tecnológica? *Dirección General de Justicia y Consumidores: Data Protection Reform.* Disponible en: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41597.

Kahneman, Daniel y Tversky, Amos (1984). Choices, values, and frames, *American Psychologist, 39*(4), 341-350. doi: http://dx.doi.org/10.1037/0003-066X.39.4.341.

Kalyvas, James R. y Overly, Michael R. (2014). *Big Data: A business and legal guide*. Nueva York: Taylor & Francis Group.

Karppi, Tero (2011). Digital suicide and the biopolitics of leaving Facebook, *Transformations: Journal of Media and Culture, 20*. Disponible en: http://www.transformationsjournal.org/wp-content/uploads/2016/12/Karppi_Trans20.pdf.

Karppi, Tero y Crawford, Kate (2016). Social Media, Financial Algorithms and the Hack Crash, *Theory, Culture and Society, 33*(1): 73-92. doi: https://doi.org/10.1177/0263276415583139.

Klaehn, Jeffery; Broudy, Daniel; Fuchs, Christian; Godler, Yigal; Zollmann, Florian; Chomsky, Noam; Pedro-Caraña, Joan; Mills, Tom y Boyd-Barret, Oliver (2018). Media Theory, Public Relevance and the Propaganda Model Today, *Media Theory, 2*(2): 164-191. Disponible en: http://journalcontent.mediatheoryjournal.org/index.php/mt/article/view/67.

Kosinski, Michal; Stillwell, David y Graepel, Tore (2013). Private traits and attributes are predictable from digital records of human behavior, *Proceedings of the National Academy of Sciences of the United States of America, 110*(15): 5802-5805. Doi: https://doi.org/10.1073/pnas.1218772110.

Kroll, Joshua A; Huey, Joanna; Barocas, Solon; Felten, Edward W; Reidenberg, Joel R.; Robinson, David G. y Yu, Harlan (2017). Accountable algorithms, *University of Pennsylvania Law Review, 165*: 633. Disponible en: https://heinonline.org/HOL/LandingPage?handle=hein.journals/pnlr165&div=20&id=&page=&t=1558886997.

Laney, Douglas (2001). *Application delivery strategies. File 949. 3D data management: Controlling data, volume, velocity and variety*. Stanford: Meta Group Research Note. Disponible en: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Lanier, Jaron (2018). *Ten Arguments for Deletting Your Social Media Accounts Right Now*. Nueva York: Henry Holt and Company.

Lawrence, Regina G. (2000). Game-Framing the Issues: Tracking the Strategy Frame in Public Policy News, *Political Communication, 17*(2): 93-114. doi: https://doi.org/10.1080/105846000198422.

Lesk, Michael (1997). *How Much Information Is There In the World?* Lesk Home Page [Página web]. Disponible en: http://www.lesk.com/mlesk/ksg97/ksg.html.

Li, Linjing; Wang, Yang; Zeng, Daniel Danjun y Yuan, Yong (2013). On the effectiveness of online big data advertising, *Proceedings of WITS 2013 - 23rd Workshop on Information Technology and Systems: Leveraging Big Data Analytics for Societal Benefits*. Disponible en: http://www.scopus.com/inward/record.url?scp=84907419115&partnerID=8YFLogxK.

Lin, Tom C. W. (2012). Too Big to Fail, Too Blind to See, *Mississippi Law Journal, 80*(2010): 355. Disponible en: https://ssrn.com/abstract=2040921.

Lippmann, Walter (1998). *Public Opinion*. Nuevo Brunswick, Londres: Transaction Publishers.

Liu, Pan y Yi, Shu-Ping (2017). Pricing policies of green supply chain considering targeted advertising and product green degree in the Big Data environment, *Journal of Cleaner Production, 164*(2017): 1614-1622. doi: http://dx.doi.org/10.1016/j.jclepro.2017.07.049.

MacAskill, Ewen (10 de junio de 2013). Edward Snowden, NSA files source: 'If they want to get you, in time they will', *The Guardian*. Disponible en: https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why.

MacKinnon, Catharine (1989). *Toward a Feminist Theory of the State*. Cambridge: Harvard University Press.

Manovich, Lev. 'Trending: the promises and the challenges of big social data'. En: Gold, Matthew K. (2012). *Debates in the digital humanities*. Arizona: University of Minessota Press.

Marsland, Setphen (2015). *Machine Learning: An Algorithmic Perspective*. Boca Ratón: CRC Press.

Martí, José Luis. 'Republican Freedom, Nondomination, and Global Constitutionalism'. En: Uitz, Renáta (2015). *Freedom and Its Enemies: The Tragedy of Liberty*. La Haya: Eleven.

Martí, José Luis y Seleme, Hugo (2015). Three comments on Philip Pettit's On the People's Terms, *Philosophy and Public Issues (New Series), 5*(2): 25-42.

Marwick, Alice y Lewis, Rebecca (2017). Media Manipulation and Disinformation Online, *Data & Society Research Institute*. Disponible en: https://datasociety.net/output/media-manipulation-and-disinfo-online/.

Mattelart, Armand y Vitalis, André (2015). *De Orwell al Cibercontrol*. Barcelona: Editorial Gedisa.

Mayer-Schönberger, Viktor y Cukier, Kenneth (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. Boston, Nueva York: Houghton Mifflin Harcourt.

McChesney, Robert W. (2013*). Digital Disconnect. How Capitalism is Turning the Internet Against Democracy*. Nueva York: The New Press.

Mendiratta, Arnav; Wong, Steve; Grimm, Reinhard; Yogeshwar, Jay y Archiquette, Shane (2015). Big data analysis for effective monetization of over the top TV content, *SMPTE 2015 Annual Technical Conference and Exhibition, SMPTE 2015*. Disponible en: https://www.scopus.com/record/display.uri?eid=2-s2.0-84963665058&origin=resultslist.

Milan, Stefania (2013). *Social Movements and Their Technologies: Wiring Social Change*. Nueva York: Palgrave Macmillan.

Mill, John Stuart (1992). *On liberty and other essays* [Editado con Introducción de John Gray]. Nueva York: Oxford University Press.

Millett, Kate (1970). *Sexual Politics*. Nueva York: Doubleday.

Minelli, Michel; Chambers, Michele y Dhiraj, Ambiga (2013). *Big data, big analytics: Emerging business intelligence and analytic trends for today's businesses*. Hoboken (Nueva Jersey): John Wiley & Sons. doi: 10.1002/9781118562260.

Morozov, Evgeni (2011). *The Net Delusion. The Dark Side of Internet Freedom*. Nueva York: Public Affairs.

Musiani, Francesca (2017). *Internet et vie privée*. París: UPPR Éditions.

Nair, Lekha R;, Shetty, Sujala, D. y Shetty, Siddhant Deepak (2017). Streaming big data analysis for real-time sentiment based targeted advertising, *International Journal of Electrical and Computer Engineering, 7*(1): 402-407. doi: 10.11591/ijece.v7i1.pp402-407.

Neff, Gina y Nagy, Peter (2016). Automation, Algorithms, and Politics | Talking to Bots: Symbiotic Agency and the Case of Tay, *International Journal of Communication, 10*(2016): 4915-4931. doi: 1932–8036/20160005.

Newell, Bryce Clayton (2014). Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control, *Government Information Quarterly, 31*(3): 421-431. doi: http://dx.doi.org/10.1016/j.giq.2014.04.001.

O'Neil, Cathy (2016). *Weapons of Math Destruction. How big data increases inequality and threatens democracy*. Nueva York: Penguin Random House.

Pasquale, Frank (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Pateman, Carole (1989). *The Disorder of Women: Democracy, Feminism, and Political Theory*. Stanford: Stanford University Press.

Pettit, Philip (1996). Freedom as antipower, *Ethics, 106*(3): 576-605. Disponible en: https://www.jstor.org/stable/2382272.

Pettit, Philip (1997). *Republicanism. A theory of freedom and government*. Oxford: Oxford University Press.

Pettit, Philip. 'Civic Republican Theory'. En: Martí, José Luis y Pettit, Philip (2010). *A Political Philosophy in Public Life: Civic Republicanism in Zapatero's Spain*. Princeton: Princeton University Press.

Pettit, Philip (2012). *On the people's terms. A Republican Theory and Model of Democracy*. Nueva York: Cambridge University Press.

Privacy International (2019) [Página web]. Disponible en: https://privacyinternational.org/es.

Public Data Lab (2019) [Página web]. Disponible en: https://publicdatalab.org/.

Puschmann, Cornelius and Burgess, Jean (2014). Metaphors of Big Data, *International Journal of Communication, 8*(2014): 1690-1709. Disponible en: http://ijoc.org/index.php/ijoc/article/view/2169.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32016R0679.

Richardson, Janice (2016). *Law and the Philosophy of Privacy*. Londres: Routledge.

Roberts, Andrew (2015). A Republican Account of the Value of Privacy, *European Journal of Political Theory, 14*(3) 320-344. doi: https://doi.org/10.1177/1474885114533262.

Roberts, Andrew (2018). Why Privacy and Domination? *European Data Protection Law Review, 1*(4): 5-11. doi: https://doi.org/10.21552/edpl/2018/1/4.

Rosenberg, Matthew; Confessore, Nicholas y Cadwalladr, Carole (17 de marzo de 2018) How Trump Consultants Exploited the Facebook Data of Millions, *The New York Times*. Disponible en: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Sarigol, Emre; Garcia, David y Schweitzer, Frank (2014). Online Privacy as a Collective Phenomenon, *COSN '14 Proceedings of the second ACM conference on Online social networks:* 95-106. doi: https://doi.org/10.1145/2660460.2660470.

Sarker, Abeed; Ginn, Rachel; Nikfarjam, Azadeh; O'Connor, Karen; Smith, Karen; Jayaram, Swetha; Upadhaya, Tejaswi y Gonzalez, Graciela (2015). Utilizing social

media data for pharmacovigilance: A review, *Journal of biomedical informatics, 54*(2015): 202-212. doi: https://doi.org/10.1016/j.jbi.2015.02.004.

Schwartz, Paul M. (2013). The EU-US privacy collision: A turn to institutions and procedures, *Harvard Law Review, (126)*7: 1966-2009. Disponible en: http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_schwartz.pdf.

Semetko, Holi A. y Valkenburg, Patti M. (2000). Framing European Politics. A Content Analysis of Press and Television News, *Journal of Communication*, *50*(2): 93-1009. doi: https://doi.org/10.1111/j.1460-2466.2000.tb02843.x.

Shalev-Shwartz, Shai y Ben-David, Shai (2014). *Understanding Machine Learning: From theory to Algorithms*. Nueva York: Cambridge University Press.

Solove, Daniel J. (2008). *Understanding Privacy*. Cambridge: Harvard University Press.

Solove, Daniel J. (2011). *Nothing to Hide. The False Tradeoff Between Privacy and Security*. New Haven, Londres: Yale University Press.

Solove, Daniel J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7): 1880-1903. Disponible en: http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf.

Sorkin, Andrew Ross (2009). *Too big to fail. The inside story of how Wall Street and Washington fought to save the financial system –and themselves*. Nueva York: Viking.

Special Eurobarometer 431 (Junio de 2015). "Data Protection" Report. Survey requested by the European Commission, Directorate-General for Justice and Consumers and co-ordinated by the Directorate-General for Communication. Disponible en: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf.

Spicer, André (2005). The political process of inscribing a new technology, *Human Relations, 58*(7): 867-890. doi: https://doi.org/10.1177/0018726705057809.

Stahl, William A. (1995). Venerating the Black Box: Magic in Media Discourse on Technology, *Science, Technology and Human Values, 20*(2): 234-258. Disponible en: http://www.jstor.org/stable/689992.

Stillwell, David J. y Kosinski, Michal (2012). myPersonality project: Example of successful utilization of online social networks for large-scale social research, *Proceedings of the 1st ACM Workshop on Mobile Systems for Computational Social Science (MobiSys).* Disponible en: https://www.gsb.stanford.edu/sites/gsb/files/conf-presentations/stillwell_and_kosinski_2012.pdf.

Taddicken, Monika (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure, *Journal of computer-mediated communication, 19*(2): 248-273. doi: https://doi.org/10.1111/jcc4.12052.

Tratado de Funcionamiento de la Unión Europea (2012/C 326/01). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:C2012/326/01.

Tufekci, Zeynep (2014). Big questions for social media big data: Representativeness, validity and other methodological pitfalls, *Procedings of the 8th Intl AAAI Conferece on weblogs and social media*. Disponible en: https://arxiv.org/abs/1403.7400.

Tufekci, Zeynep (2017). *Twitter and the tear gas. The power and fragility of networked protest*. New Haven, Londres: Yale University Press.

Turow, Joseph; Hennessy, Michael y Draper, Nora (2015). The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation, *A Report from the Annenberg School for Communication University of Pennsylvania*. Disponible en: https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

van Der Sloot, Bart (2018). A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle, *Computer Law & Security Review, 34*(3): 539-549. doi: https://doi.org/10.1016/j.clsr.2017.11.013.

Ward, Jonathan Stuart y Barker, Adam (2013). Undefined by Data: A Survey of Big Data Definitions, *Cornell University*. Disponible en: http://arxiv.org/abs/1309.5821.

Warren, Samuel D. y Brandeis, Louis D. (1890). The Right to Privacy, *Harvard Law Review, 4*(5): 193-220. doi: 10.2307/1321160. Disponible en: https://www.jstor.org/stable/1321160.

Young, Iris Marion. 'Impartiality and the Civic Public'. En: Benhabib, Seyla y Cornell, Drucilla (eds.) (1987). *Feminism as Critique. On the politics of Gender*. Minneapolis: University of Minnesota Press.

Youyou, Wu; Kosinski, Michal y Stillwell, David J. (2015). Computer-based personality judgments are more accurate than those made by humans, *Proceedings of the National Academy of Sciences of the United States of America, 112*(4): 1036-1040. doi: https://doi.org/10.1073/pnas.1418680112.

Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Nueva York: Public Affairs.

Big data, poder y libertad. Sobre el impacto social y político de la vigilancia masiva.

Big data, power and freedom. On the social and political impact of massive surveillance.

Tesis doctoral presentada en la Universitat Pompeu Fabra el año 2019.

upf.

TESI DOCTORAL UPF / 2019