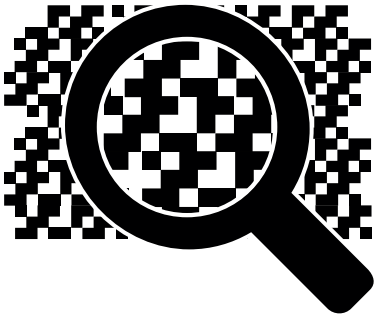
TECNOLOGÍA

ROSA COLMENAREJO FERNÁNDEZ

UNA ÉTICA PARA BIG DATA

INTRODUCCIÓN A LA GESTIÓN ÉTICA DE DATOS MASIVOS

Prólogo de Marta Pedrajas



EDITORIAL UOC

Una ética para *big data*

Introducción a la gestión ética de datos masivos

Rosa Colmenarejo Fernández

Prólogo de Marta Pedrajas

EDITORIAL UOC

Director de la colección Manuales (Tecnología): Antoni Pérez

Diseño de la colección: Editorial UOC
Diseño de la cubierta: Natàlia Serrano

Primera edición en lengua castellana: julio 2017
Primera edición digital: octubre 2017

© Rosa Colmenarejo Fernández, del texto

© Editorial UOC (Oberta UOC Publishing, SL), de esta edición, 2017
Rambla del Poblenou, 156
08018 Barcelona
http://www.editorialuoc.com

Realización editorial: Sònia Poch

ISBN: 978-84-9116-941-3

Ninguna parte de esta publicación, incluyendo el diseño general y de la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma ni por ningún medio, ya sea eléctrico, químico, mecánico, óptico, de grabación, de fotocopia o por otros métodos, sin la autorización previa por escrito de los titulares del *copyright*.

Autora

Rosa Colmenarejo Fernández

Doctora por la Universidad de Córdoba. Su línea de investigación principal está centrada en la caracterización de una ética de la emancipación, a partir del desarrollo de capacidades que facilitan las oportunidades que ofrecen la cultura y la tecnología. Es máster en Métodos de investigación en economía y empresa, licenciada en Humanidades, en el itinerario de Filosofía, por la Universidad de Córdoba e ingeniera por la Universidad Politécnica de Madrid. Experta universitaria en Gestión del patrimonio cultural y natural por la Universidad Internacional de Andalucía, y miembro de la red de expertos en patrimonio de las universidades andaluzas. Ha realizado estancias de investigación en la Universidad Centroamericana (UCA) en Managua y en la Universidad Nacional Autónoma (UNAN) en León, Nicaragua; en el Institute of Development Policy and Management de la Antwerp University, Bélgica; en la Georgetown University, Estados Unidos; y en el Centro de Estudos Sociais de la Universidade de Coimbra, Portugal. Desde 2013 es profesora contratada del Departamento de Humanidades y Filosofía de la Universidad Loyola Andalucía.

A Manuela y Gonzalo,
a Rafael,
por su amor.

Gracias a José Ramón Rodríguez, Montse Serra y Javier Sánchez
por su amistad y apoyo.

Índice

Prólogo 13
Marta Pedrajas

Capítulo I. Ética, internet de las cosas y *big data* ... 19
1. Introducción 19
2. ¿Dónde ubicar una ética de los *big data*? 23
3. El problema del sujeto moral 25
3.1. Ética y moral: caracterización del sujeto moral precomputacional 26
3.2. ¿Necesitamos pensar la ética de otro modo cuando pretendemos aplicarla al escenario de la IoT? 30
Bibliografía 35

Capítulo II. ¿Qué debo hacer? ¿Lo bueno, lo justo o lo correcto? Teorías éticas y principios profesionales 39
1. Introducción 39
2. Teorías éticas. Breve introducción 41
3. Un apunte sobre la condición inherentemente política de la tecnología 44
4. Principios orientadores de la acción del buen profesional 47
4.1. Principio de beneficencia 49
4.2. Principio de autonomía 51
4.3. Principio de no-maleficencia 54

4.4. Principio de justicia 57
Bibliografía..... 59

Capítulo III. Problemas éticos fundamentales que afectan a la gestión de *big data* 63
1. Introducción..... 63
2. Identidad..... 64
3. Vulnerabilidades visibles e invisibles de la privacidad en el contexto de *big data*..... 70
4. Propiedad de los datos: ¿derecho o interés? 78
5. Hacia una gestión de la privacidad justa y equitativa: entre la ética y la ley 79
Bibliografía..... 87

Capítulo IV. La toma de decisiones éticas en el entorno de la IoT y *big data* 91
1. Introducción..... 91
2. Aplicación de la teoría de los *stakeholders* a la toma de decisiones en el entorno de la IoT y *big data*..... 94
3. La toma de decisiones éticas y sus implicaciones.. 98
4. Puntos de decisión ética: un marco para la toma de decisiones 102
Bibliografía..... 107

Capítulo V. La regulación de los sistemas de *big data* e inteligencia artificial..... 111
1. Introducción..... 111
2. Preparando las sociedades para el futuro: propuestas desde Estados Unidos 115
3. Regulación de algoritmos y robots: propuestas desde la UE 118

4. Código de ética y conducta profesional
de la Association for Computing Machinery..... 121
5. La sociedad civil: *hackers*, ONG..... 124
Bibliografía..... 127

Prólogo

Decía Ortega y Gasset que la misión de la universidad era la búsqueda de la verdad, la transmisión del saber a las generaciones siguientes y la discusión abierta y crítica en una comunidad de quienes aspiran a la verdad. A todo ello deberíamos añadir también que la universidad debe proporcionar a la sociedad no solo conocimientos, sino también la sabiduría necesaria para buscar el bien común y la justicia. Los tiempos no han cambiado tanto y la *revolución de las masas* bien podría ser la *revolución de los datos masivos*, del *big data*. A los que hay que afrontar con las mismas armas de la historia, las que nos da la ética desde los tiempos de los clásicos: reflexión, cuidado del sujeto, la persona en el centro y búsqueda del bien común. Así tienen pleno sentido la tecnología, la ciencia, la economía, la informática y cualquier revolución que se produzca. Porque lo contrario es ser corto de miras, diría Kant, pues no solo hay que tener una mirada ética por justicia, sino también por egoísmo inteligente, y al menos por el bien propio habría que tener en cuenta ciertos principios éticos para la convivencia común.

Pero en tiempos de modernidad líquida y pensamiento débil, los datos pueden tomar un lugar que no les corresponde: ser fin y no medios. Y los datos son un medio, un medio impresionante por sus posibilidades y su alcance, por la información que proporcionan y por los canales de participación

que habilitan. Es todo un desafío para las democracias y por primera vez en la historia tenemos la posibilidad de construir sociedades inclusivas en las que nadie se quede atrás, dando voz a los ciudadanos, también a los más alejados, hasta llegar a los más vulnerables, porque ahora su opinión cuenta. Pero no cuenta de cualquier modo, hay rostros, voz y miradas detrás de estos datos y es, por tanto, no solo una labor ética su obtención, sino sobre todo su utilización, porque la información sigue siendo *poder*, y la información del *big data* es *más poder*, si cabe. Por lo que el respeto al sujeto, su identidad y privacidad, debe ser máximo. Como máxima y poderosa también es la fuerza que emana de la justicia y la búsqueda del bien común. Muchas personas, instituciones y organizaciones a lo largo de la historia han tenido como objetivo y prioridad construir sociedades justas y solidarias, donde las libertades y derechos fueran respetados y el desarrollo compartido. Teniendo en cuenta además a las generaciones futuras, ahora el desarrollo es, sobre todo, un desarrollo humano y sostenible. Es nuestro futuro común. Y en este futuro común la tecnología nos proporciona los medios, el *cómo*; pero los *fines* siguen siendo las grandes preguntas del ser humano: ¿qué puedo conocer?, ¿qué debo hacer? Y como bien expone la autora en el libro, la gran pregunta ahora sería: ¿cuáles son nuestros objetivos como humanidad? Para Naciones Unidas (ONU) el bien común ha tomado forma de desarrollo sostenible en la agenda 2030 y en los diecisiete *Objetivos de Desarrollo Sostenible* que abarcan las cinco grandes prioridades: personas, planeta, prosperidad, paz y alianzas entre todos para lograrlo.

En este marco, el *big data* juega un papel fundamental, es un instrumento poderoso y un medio indispensable para lograr este desarrollo sostenible, este bien común, y por eso

desde hace años en todos los foros internacionales se habla de la necesidad de una *revolución en los datos* al servicio de la erradicación de la pobreza extrema y del hambre, de la disminución de las desigualdades, del acceso al agua y la energía, del fomento de los derechos y libertades, del empoderamiento de las niñas y de las mujeres, de la protección del planeta, de los bosques y los océanos, en definitiva, del logro de la paz. Y, además, en este viaje común, todos los países de la ONU sin excepción se han comprometido a que *nadie se quede atrás*. Para lograrlo —la identificación de las minorías, de los excluidos y de los marginados de todas las sociedades— es más necesaria que nunca la revolución de los datos; es el primer paso.

Este libro es imprescindible por su contenido, y es acertadísimo el momento en el que aparece. Su autora, Rosa Colmenarejo, filósofa comprometida con el bien común y la justicia, nos ofrece las claves necesarias para afrontar esta revolución en los datos con una mirada ética que compromete a la tecnología y a las personas en su obtención y utilización. Colmenarejo nos ofrece numerosas claves para repensar el sujeto, para reconstruir la identidad más allá de algoritmos. A través de los principios éticos que nos ofrece, superando el *business ethics*, pero recogiendo lo mejor de la modernidad, reconstruimos al sujeto dueño de su vida y de su futuro, así como del sujeto de la humanidad. La ética aplicada al más alto nivel, a lo que en la ONU se conoce como *cuestiones frontera*: los sistemas de información, el internet de las cosas (IoT), la inteligencia artificial, el *big data*. En resumen, la autora nos proporciona un impulso, un acelerador de primer orden de la agenda de la ONU, de la agenda de desarrollo sostenible.

Este libro nos da muchas claves, pero es sobre todo la mirada ética que propone la autora la que nos presenta el *big*

data como una gran oportunidad para tomar mejores decisiones, basadas en mejores datos, y evolucionar de los grandes beneficios privados a la prosperidad compartida; pasar del control y seguridad internacional a la paz sostenida; de la manipulación de la naturaleza al desarrollo sostenible; de la indiferencia frente a los marginados a encontrarlos, verlos e incluirlos en el desarrollo humano global; y pasar de sociedades desiguales e injustas a construir sociedades de encuentro, equitativas y solidarias. El *big data* puesto al servicio de los bienes de la humanidad es lo que nos ofrece la autora. No puede haber una hoja de ruta mejor y más necesaria para el mundo actual, para construir nuestro futuro común.

Marta Pedrajas
Doctora en Filosofía. Especialista en Políticas de desarrollo del Programa de Naciones Unidas para el Desarrollo (PNUD).

La ley no reemplaza a la conciencia.

Edward Snowden

Capítulo I
Ética, internet de las cosas y *big data*

1. Introducción

Desde que Boyd y Crawford (2012) planteasen sus *Critical Questions for Big Data* quedó en evidencia algo que ya se vino anunciando a lo largo del siglo XX, esto es, la necesidad urgente de desarrollar una ética[1] adaptada a los cambios que provocarían los avances tecnológicos sobre la calidad y las formas de vida (Eco, 1973; Jonas, 1970; Ortega y Gasset, 1939). Efectivamente, las sociedades actuales han entrado en una dinámica de cambio constante, en gran parte motivada por la eclosión de información que el uso masivo de tecnología genera al minuto. Entendemos aquí las sociedades no como «comunidades que comparten valores e intereses» sino como «estructuras sociales contradictorias surgidas de conflictos y negociaciones entre diversos actores sociales, en muchos casos opuestos» (Castells, 2009, pág. 38). Los *big data* (BD), como parte de la denominada *internet de las cosas* (IoT, por sus siglas en inglés), deben ser considerados un fenómeno sociotecnológico en tanto que no solo están transformando la cultura de comunicación entre seres humanos,

1 La ética, tanto personal como organizacional, consiste en la adquisición de experiencias y conocimientos sobre la realidad que van conformando nuestro carácter o cultura, en el caso de las organizaciones. Este *carácter ético* nos asiste en la toma de decisiones orientadas hacia el bien, no solo en un momento determinado sino en el conjunto de la vida.

sino que intervienen simultáneamente en los espacios público y privado de los agentes haciendo que la frontera entre ambos se muestre más difusa que nunca antes.[2]

Las estructuras sociales que comienzan a manifestarse a partir de la gestión, disponibilidad y uso de los BD, hacen emerger conflictos éticos en muchos casos heredados de la ética de los negocios, aunque ahora esta se vea superada por las circunstancias en las que operan la generación y gestión masiva de datos. Y ello, precisamente, por aquello que les caracteriza, esto es, las denominadas *5V*: volumen, velocidad, variedad, veracidad y valor (Laney, 2001; Beyer, Laney, 2012; Hashem *et al.*, 2015). La *business ethics* es una disciplina que lleva décadas de ventaja en la resolución del conflicto sobre si se deben confiar las decisiones éticas que afectan a la empresa y al resto de sus grupos de interés, únicamente a los criterios morales de sus directivos y/o empleados, o si, además, la empresa debe desarrollar una cultura ética específica que asista en la toma de decisiones. En tanto que almacenar, gestionar y utilizar datos (en muchos casos con

2 Consideramos aquí que lo que se denomina *internet of things* (IoT) consiste básicamente en: i) una tecnología sensible inserta en entidades físicas, objetos cotidianos de uso generalizado, que recopila datos de forma constante; ii) redes que permiten el intercambio de los datos generados por esta tecnología; iii) potencia computacional para la interpretación de esta ingente cantidad de datos (*big data*); y, finalmente, iv) agentes que reaccionan ante los resultados procesados, de nuevo insertados en los objetos tecnológicos cotidianos. Los *big data* forman parte del sistema que conforma la IoT, pero en tanto que esta última se estructura en torno a los datos, algunos autores consideran ambos conceptos como «las dos caras de la misma moneda». En este trabajo se consideran así, de modo indistinto, una ética para *big bata* y una ética aplicada a la IoT. Véase «Big Data and the Internet of Things: Two Sides of the Same Coin?», Tamara Dull, *SAS Best Practices*: <http://www.sas.com/en_us/insights/articles/big-data/big-data-and-iot-two-sides-of-the-same-coin.html>

fines lucrativos) plantea renovados problemas relacionados con la privacidad, la propiedad, la identidad, la confianza o la reputación, ya no es posible eludir los componentes éticos de esta novísima acción humana relacionada con los datos. Estamos ante nuevos escenarios que obligan a pensar la ética de una forma necesariamente revolucionaria, un pensamiento moral que ponga en crisis la ética aplicada tal y como la venimos entendiendo desde la eclosión de la *business ethics*, esto es, como una disciplina diferenciada de la actividad propia de la empresa o de las organizaciones en vez de ser parte integral e indiferenciada de estas. En este trabajo nos posicionamos en la segunda de las opciones.[3]

Quizá hayamos ido ya demasiado lejos en el planteamiento del objeto de esta introducción, porque ¿a quién nos referimos cuando hablamos de *sujeto moral*? ¿Dónde nos ubicamos cuando utilizamos el término ética? ¿Está relacionado con la *moral* o, más bien, con la *legalidad*? ¿Solo es *incorrecto* aquello que está prohibido por ley? ¿Qué aspectos del ejercicio profesional relacionado con los BD tienen grandes dificultades para llegar a estar regulados legalmente? ¿Es lo mismo *bueno* que *correcto*?

3 Nos referimos a la incorporación de la responsabilidad social corporativa (RSC) como una obligación adicional al cumplimiento tanto de la norma legal como de los objetivos fijados por la junta de accionistas. Una obligación que no es tal porque la característica fundamental de la RSC es la aplicación voluntaria de sus principios, pero que se adopta en tanto que se considera útil para favorecer la reputación y con ello la confianza de consumidores, clientes y/o proveedores. Esta concepción utilitarista de la ética como «inversión rentable» se aleja de la necesaria incorporación de la ética a la cultura de la empresa y las organizaciones, pues del mismo modo que los (buenos) hábitos conforman el carácter y con ello la moral de las personas, las (buenas) prácticas deberían conformar una cultura empresarial orientada hacia el bien en el más amplio sentido del término.

Hay dos problemas fundamentales que deben ser confrontados por una ética aplicada a la denominada IoT: i) determinar en qué realidad se ubica este campo de reflexión ética; e ii) identificar al sujeto o sujetos a quienes se podrán atribuir tanto la toma de decisiones como la responsabilidad que de ellos puedan derivarse (Popescul; Georgescu, 2014).

Estas son las dos cuestiones que intentaremos atender en este primer capítulo. Nos ocuparemos primero de delimitar las áreas en las que podemos establecer que opera esta ética aplicada a la IoT. Para ello nos situaremos en el marco más amplio que nos facilita lo que se ha denominado una *taxonomía* de la ética aplicada a los sistemas de información, aunque dicha clasificación sea aún polémica (Ess, 2006; 2009). Argumentaremos inmediatamente después, siquiera superficialmente, sobre aquello que distingue la ética de la *moral*, y cómo se conectan ambas disciplinas, pues son uno de los pilares fundamentales en los que se asienta toda vida social «bien orientada», por emplear un concepto aristotélico y comenzar a entrar ya en materia. Ello nos permitirá comprender el sentido de aquello que denominamos *sujeto moral*.

Así, aunque es habitual el uso indiferenciado de los términos ética y *moral*, es cierto que en muchas ocasiones hemos escuchado a nuestros estudiantes y colegas expresar esta duda respecto a cómo diferenciar ambos, cuestionando incluso la necesidad de tal distinción. El problema no parece residir, sin embargo, en distinguir uno de otro, sino más bien en no comprender el sentido de ninguno de los dos. El cumplimiento de este primer doble objetivo nos ayudará después a plantear inmediatamente unas conclusiones que apuntarán hacia una

primera justificación sobre la necesidad de desarrollar una ética para el escenario que emerge de la recopilación, almacenamiento, gestión y uso de los BD.

2. ¿Dónde ubicar una ética de los *big data*?

Es posible considerar la filosofía de la IoT, o de los *big data*, en tanto consideramos el fenómeno como un paradigma más que un mero *cambio tecnológico* (Barocas; Nissenbaum, 2014), como aquella que trata la conceptualización de términos y definiciones (ontología), los métodos empleados para la obtención de conocimiento, dentro de un determinado marco hermenéutico que maneja unas ideas concretas de verdad y objetividad (epistemología) así como la observación de las consecuencias (ética) que supone la obtención, disposición, uso y extracción de información mediante la gestión de las colecciones masivas de datos (BD) que se obtienen en el espacio de la IoT. Así, ontología y epistemología pueden considerarse en un nivel *interno* a esta ciencia de los datos (Floridi, 1999); mientras la ética es *externa*, pues se ocupa de las consecuencias de la actividad a la que dan soporte, siquiera teórico, las dos primeras, tanto en individuos, organizaciones, comunidades o sociedad en general (Swan, 2015).

La ética aplicada a la IoT puede considerarse una ética de ámbito profesional en tanto que se ocupa esencialmente de la responsabilidad de determinados grupos de expertos, pero también tendría una parte de ética empresarial en tanto que dichos expertos trabajan en corporaciones de ámbito privado o público que deben desarrollar una determinada

cultura ética que les permita tomar decisiones orientadas hacia el interés general de la sociedad o bien común;[4] del mismo modo, vertebrar eficazmente una ética cívica en un contexto de interacción intercultural, fragmentación social y exclusión ayudará a una reformulación de qué pueda ser ese *bien común*, en cuanto que ha de interpretar los desafíos y exigencias actuales atendiendo, entre otros, a la expansión y la consolidación de la racionalidad científica y tecnológica a escala planetaria, con la explotación de los recursos naturales, o con la pluralidad de identidades religiosas e ideológicas (Michelini, 2008; Zamagni, 2008). Aunque en ella operan necesariamente, además, problemas y reflexiones propios de la ética de los sistemas de información, es decir, aquella que tiene por objeto la representación, organización, clasificación, recuperación, disponibilidad, preservación, circulación y uso de la información en relación con el medio digital.[5]

La reflexión ética que corresponde a esta IoT podría mapearse de acuerdo con la siguiente taxonomía: i) la *ciberética* se ocupa de analizar los modos en los que internet está condicionando la comunicación social entre individuos y organizaciones. En esta podría incluirse, por tanto, la ética

4 *Bien común* puede establecerse como aquello opuesto a *propio*, del mismo modo que *público* se opone a *privado*. Seguimos aquí a Hannah Arendt, quien en *La condición humana* (1958) estableció: «Todo lo que aparece *en público* puede ser visto u oído por todos»; y, por otra parte, «el mundo mismo en cuanto es *común* a todos y distinto del espacio que cada uno de nosotros ocupa privadamente». Por esto convenimos que lo *común* es el lugar de lo que no es propio, es decir, el lugar de las relaciones interpersonales, que no es sino el espacio natural de la ética (Arendt, 2015, pág.78).

5 Ver documentación disponible en apartado «Publicaciones» de la página web del International Center for Information Ethics: <http://icie.zkm.de/publications>

de las redes sociales, la ética de la IoT e incluso la ética aplicada a la robótica. Se han identificado tanto unos valores que operan de forma positiva en este campo, como la libertad de expresión o el desarrollo de procesos democráticos participativos, y otros negativos como la vigilancia masiva y el control que pueden llevar a la exclusión o la censura. La ciberética sería una «teoría sobre la libertad en el medio digital» (Capurro *et al.*, 2013); ii) la ética de la computación comparte espacios con la ciberética, en tanto que se ocupa de la tecnología que se emplea para la recopilación, gestión y tratamiento de los datos, pero sin ceñirse a internet, es decir, se ocupa de los problemas éticos que surgen en el desarrollo y utilización de herramientas computacionales en todos los ámbitos de la sociedad (Johnson, Miller, 2009; Stahl *et al.*, 2016); y iii) la ética de la información en investigación biomédica, como parte de la bioética, que sería aquella que se ocupa de analizar la interacción entre seres vivos y tecnologías digitales y/o computacionales, pero sin ceñirse únicamente a la obtención y gestión de datos obtenidos mediante un acto médico, sino también de los biométricos obtenidos con fines de vigilancia y seguridad (Bietz *et al.*, 2016; Kokumai, 2016; Sharon, 2016; Stylianou, Talias, 2017).

3. El problema del sujeto moral

Los ciudadanos ya no pactamos las condiciones de nuestra seguridad con el estado, como dejó planteado Hobbes en su *Leviatán* (1651), sino con nuestro proveedor de datos, quien

nos da acceso a la sociedad red.[6] La cuestión estriba ahora en estimar el alcance de nuestro acceso a las cláusulas de dicho contrato y en dilucidar si nuestra posición como *sujetos morales* es bien como profesionales, ciudadanos/as o como clientes y/o proveedores. ¿Quién debe asumir entonces la condición de sujeto moral en la ética de los BD? Todo apunta hacia una combinación, ineludible e indisoluble, de todos ellos.

3.1. Ética y moral: caracterización del sujeto moral precomputacional

Los seres humanos somos seres tan inherentemente sociales como morales. Ello explica que precisemos acordar normas básicas de convivencia, siquiera implícitas, que nos permitan llevar una vida buena, una vida orientada hacia la felicidad. Esta idea de *telos* procede de la Ética *nicomaquea*, escrita por Aristóteles en el siglo IV a. C. y debe ser comprendida en su justa medida, porque efectivamente, ideas de *felicidad* puede haber tantas como personas. Por *felicidad* podemos comprender bienestar, autorrealización, alcanzar aquellas metas, en fin, ya que todas y cada una de las personas tienen razones para valorar como «convenientes» con la meta de conformar su

6 Véase el discurso plenamente político de Mark Zuckerberg con motivo de su nombramiento como doctor *honoris causa* de la Universidad de Harvard, reclamando la construcción de un nuevo *pacto social* que busque combatir la desigualdad y evite asumir riesgos en nombre de la innovación. «Mark Zuckerberg tells Harvard grads that automation will take jobs, and it's up to millennials to create more», Hayley Tsukayama, *The Washington Post*, 25 de mayo de 2017: <https://www.washingtonpost.com/news/the-switch/wp/2017/05/25/mark-zuckerberg-tells-harvard-grads-that-automation-will-take-jobs-and-its-up-to-millennials-to-create-more/?utm_term=.2df220fa4edc>

propio proyecto de vida. La condición inherentemente social de los seres humanos supone una necesidad y una esperanza en la comunidad dentro de la que nos insertamos. A pesar de que la idea de sociedad como suma de individuos que subyace en las propuestas contractualistas más incipientes de Hobbes[7] o Rousseau, en su *El contrato social* (1762), es aún ampliamente aceptada hoy en día, nos inclinamos aquí por la propuesta de María Zambrano, quien mantiene que abstraer al ser humano de la sociedad para insertarlo luego en ella es un error. Para Zambrano, «el ser humano está en la sociedad. Y solo en ella aparece» (Zambrano, 1987, pág. 122).

Esta idea de condición inherentemente social de los seres humanos nos puede ayudar a comprender el sentido del primer término empleado para referirse a ética. El primer *éthos* (*ἤθος*) griego, recuperado por Heidegger en su *Carta sobre el humanismo* (1958), es aquel que procede de tragedias, como las de Sófocles, y de la poesía anteriores a Platón, es decir, mucho antes de que existiese una disciplina filosófica que estudiase la ética en sí. Con *éthos* se referían a *estancia*, *morada*, *lugar donde se habita*, el contenedor que configura nuestro ser respecto al mundo (Lledó, 2015). Es en el empeño de traducir una máxima de Heráclito cuando Heidegger encuentra esta noción que podríamos denominar *espacial* de la ética: «La estancia del hombre contiene y preserva el advenimiento de aquello que le toca al hombre en su esencia» (Heidegger, 2000, págs. 72-83).

¿Cómo podría sernos útil esta noción espacial al abordar la ética de los BD? ¿Cómo, si los BD se dan en un entorno

7 Véase la ilustración que acompañó a la primera edición de su *Leviatán* (1651): una idea de estado que, adoptando la figura de un gigante, constituye en sí mismo además un paisaje compuesto por cientos de pequeños individuos.

no-físico, que en gran parte nos dificulta, si no nos evita, revelarnos como sujetos morales? Porque nuestra condición social está ligada a otra: aquella que nos hace inherentemente morales. Siguiendo a Aranguren, ante un estímulo los humanos hemos de confrontar necesariamente la realidad antes de tomar una decisión, hemos de «pararnos a pensar», detenernos a justificar nuestra acción ante un abanico de posibilidades que se ubican en la irrealidad. Dice Aranguren que la primera dimensión de la libertad en las personas se da precisamente en este liberarse del estímulo que supone la reflexión; la segunda dimensión de libertad que nos es propia se hace efectiva cuando tomamos una decisión, cuando decidimos actuar de un modo y no de otro, cuando justificamos nuestros actos. Esta es la dimensión moral que nos es inherente a todos los seres humanos. Nuestra capacidad para decidirnos entre irrealidades posibles, distinguiendo entre el bien, el mal y/o aquello que atiende exclusivamente a nuestros intereses (Aranguren, 2005).

¿Qué variables intervienen entonces en esta toma de decisiones, al menos desde una perspectiva ética? En primer lugar, se podrían considerar tanto el temperamento (*páthos*) como el talante (*héxis*), dados ambos por *naturaleza*, pero es aún más importante el *carácter*, el modo de ser que cada uno se va forjando a lo largo de su propia vida, tomando decisiones, acumulando experiencias. Esta idea de *carácter*, susceptible de ser adquirido y moldeado, es la que subyace en la acepción de ética que se corresponde con el término también griego *êthos*, y que será aquella que se popularice y gane más adeptos a partir de Aristóteles. El *êthos* es un concepto bien amplio que se podría traducir como 'modo o forma de vida'. Una forma de vida que es disposición, carácter, costumbres y que incluye, necesariamente, también, la concepción espacial que implica el

éthos. El *êthos* como carácter, como modo aprendido de vivir, procede del *éthos*, del hábito (virtudes y vicios), del lugar seguro en el que nos refugiamos mediante la repetición aprendida de nuestros actos. Ética, como combinación de ambas, es el suelo firme, que dice Aranguren, el fundamento de toda práctica, la raíz de la que brotan todos los actos humanos (Aranguren, 1994, págs. 172-177). En latín *éthos* y *êthos* fueron recogidas en el término *mos*, moral. La obra moral de una persona parece consistir, entonces, en la adquisición de un modo de ser. Una adquisición que se considera gradual, desde los sentimientos hasta el carácter, mediados por la costumbre, el hábito.

> «El vocablo *éthos* tiene un sentido infinitamente más amplio que el que damos hoy a la palabra ética. Lo ético comprende, ante todo, las disposiciones del hombre en la vida, su carácter, sus costumbres y, naturalmente, también lo moral. En realidad, podría traducirse por 'modo o forma de vida', a diferencia de simple manera» (Zubiri, 1944, pág. 259).

Estas ideas de carácter y hábito serán fundamentales para la conformación de la denominada *business ethics*, cuando se precise delimitar al sujeto moral que opera con responsabilidad en la actividad organizacional o empresarial: establecer una determinada cultura de la organización, será como moldear este carácter al que se refería Aristóteles. Esta cultura será la que establezca los hábitos y las costumbres que determinarán el comportamiento acorde a una ética de la organización, o de la empresa.

Pero, ¿qué es eso *moral* que distingue Zubiri? Siguiendo de nuevo a Aranguren y lo que llama argumento prefilosófico, «el hombre es constitutivamente moral porque es constitutivamente libre, tiene por fuerza que hacerse —suficiente o insuficientemente— su propia vida». Lo moral vendría a ser

aquello que orienta nuestras decisiones, el sentido de la vida, en la más amplia acepción del término. Aún más, la moral vendría a significar la ética vivida, *ethica utens*, la ética aplicada a la conformación del propio carácter o de la propia cultura de las organizaciones. De acuerdo con este argumento, la moral ha orientado la toma de decisiones y con ello la acción de los seres humanos mucho antes de que existiese aquella filosofía práctica denominada Ética.

La Ética, con mayúscula, podría establecerse entonces por contraposición a la anterior. Se trataría de una «ética pensada», o *ethica docens*, la disciplina que emerge a partir de Aristóteles, primero como parte de la política, pues considera, con Platón, que hay una correspondencia entre las formas éticas del *bíos* individual y las formas políticas de las *politeiai*. La ética es a partir de entonces Ética, pensamiento moral, que se ocupa de las diferentes teorías éticas que establecen las correspondientes concepciones del bien, de lo correcto, o de aquello que caracteriza al sujeto moral, pero también de las posibles taxonomías que operan dentro de la ética aplicada a una determinada disciplina. La ética que nos ocupa sería un pensamiento, una reflexión, sobre los problemas y las formas que tienen las personas de tomar decisiones en el escenario que emerge de la IoT y los BD.

3.2. ¿Necesitamos pensar la ética de otro modo cuando pretendemos aplicarla al escenario de la IoT?

Esta ética que estamos planteando, necesariamente renovada en cuanto que el sujeto moral es una extraña amalgama

de identidades y roles, es la que consideramos aquí que debe superar, en objetivos y en alcance, a una ética (meramente) aplicada a las nuevas tecnologías, que supondría a los profesionales y a las mismas máquinas como únicos sujetos morales; sino una ética de la emancipación, también de las máquinas, en la que los sistemas de valores —normas y principios morales— que la sustenten emerjan desde aquello que nos hace intrínsecamente humanos: autonomía, dignidad y solidaridad (Trías, 2000). En palabras de Judit Butler, se trataría de resaltar lo obvio, cuando lo evidente se desvanece: estamos ante un nuevo escenario que obliga a pensar la ética de una forma necesariamente revolucionaria, pues un nuevo sujeto moral, aún por definir, ha suplantado ya al sujeto —humano— responsable en la toma de decisiones.

Algunas evidencias de esta inevitable emancipación de las máquinas de aquello humano: i) las máquinas —me refiero aquí a sistemas que funcionan con algoritmos como Google, Facebook, Spotify, etc.— se han emancipado (ya) de la memoria, sometiendo nuestra memoria. Construyen y arrojan al mundo nuestra biografía, que podría llegar a conformar nuestra propia identidad, de acuerdo a parámetros que no elegimos los humanos. Los algoritmos, rediseñados cada día, eligen por nosotros los contenidos de nuestra biografía, saben más de nosotros que nosotros mismos, no solo de nuestro pasado sino, y aquí más probablemente, de nuestros deseos futuros; ii) las máquinas se han emancipado (ya) de la intuición, sometiendo nuestra intuición. No paseamos *a zonzo* las ciudades que no conocemos, sino que dejamos que una aplicación guíe nuestros pasos, nos sometemos como autómatas a un servicio «puerta a puerta». Google Maps se encarga de recordarnos que «es irresponsable [*sic*] no atender

la ruta marcada como la más rápida: provocará retenciones no previstas por el sistema»; iii) podríamos seguir enumerando, y estudiando si las máquinas se han emancipado de los cuerpos, sometiendo nuestros sentidos: gafas de realidad virtual, algunos videojuegos, etc. El problema del sujeto moral deviene entonces en ¿quién debe ser considerado sujeto de emancipación?

Derivado de este problema, surge el siguiente. El sujeto moral no puede verse reducido a un mero individuo que opera entre espacios de responsabilidad pública (Etxeberría, 2011). Las fronteras no son solo más borrosas entre espacios de responsabilidad, sino que dichos espacios se multiplican y se unifican en tanto que su porosidad y fragmentación es lo que mejor les caracteriza. Este «renovado» sujeto que emerge de la interacción con las máquinas es tan constitutivamente moral y social como su antecesor. Sigue corporeizado, aunque aún parcialmente virtualizado (Butler, 2017). Ello implica que consideramos, aún en este estadio, que en la IoT operan seres humanos que toman decisiones conscientes, ya sea programando código, algoritmos o como simples consumidores de información. Su responsabilidad, hacerse cargo de las consecuencias de tales decisiones, sigue intacta, aunque sea necesario precisar algo más sobre ella.

Este escenario promueve aquello que Bauman ha denominado «el encubrimiento tecnológico del *yo moral*», entendiendo que la función de la tecnología no es sino la fragmentación de la vida, del *yo*, en un grupo de facetas que generan problemas cada uno de los cuales requiere, a su vez, diferentes técnicas y grupos de expertos para su resolución. El *yo moral* es la víctima de esta fragmentación, en tanto que como sujeto no enfrenta nunca la totalidad, ya sea del mundo o de otro

ser humano. La consecuencia inmediata de esta parcialidad mediada por la intervención de la tecnología en la vida es el derecho que se adquiere para reclamar la inocencia moral: «El sujeto nunca actúa como una persona total, tan solo como un portador momentáneo de uno de los varios problemas que marcan su vida; tampoco actúa sobre el Otro como persona, ni sobre el mundo como totalidad». Lo que implica que no sea posible la responsabilidad, ni por ese *Otro*, ni por el mundo (Bauman, 2006, pág. 225). Esta fragmentación, en cuanto que encubrimiento de la naturaleza sistémica del *habitus* —hábitat humano— y, con ello, del desmembramiento del yo moral, es una de las principales causas de lo que Beck (1992) denominó *sociedad riesgo*, y en la que es preciso distinguir *riesgo* de *peligro*: así, riesgo pertenece al discurso de los *juegos de azar*, eludiendo la oposición entre éxito y fracaso, o entre seguridad y peligro. La sociedad riesgo es una sociedad que potencia la visión del mundo como un juego, y estar en el mundo como jugando (Douglas, 1992) .

En nuestra relación con las máquinas vamos eludiendo tomas de decisión y con ello responsabilidades, pero esto no deja de ser, como tantas veces, una forma de salvar los problemas en el corto plazo. Las decisiones éticas siguen existiendo y siguen demandando que alguien —algo— se haga cargo de la realidad a la que aluden. Recordemos a Zambrano: «El ser humano está en la sociedad. Y solo en ella aparece» (Zambrano, 1987, pág. 122). Si ubicamos esta idea en el contexto de la IoT, espacio en el que se están generando los datos, la cuestión debería plantearse de este modo: ¿Es posible abstraer al ser humano, en cuanto que sujeto, de la sociedad red, para luego insertarlo en ella única y exclusivamente cuando se producen conflictos éticos o legales?

Las máquinas están aprendiendo ahora lo que es, ¿por qué no enseñarles lo que debería ser?

> «El objetivo de la investigación en inteligencia artificial (AI) ha sido comprender los principios que subyacen en el comportamiento inteligente y aplicarlos a la construcción de máquinas capaces de presentar dicho comportamiento. En los 50 años de vida de la disciplina se han buscado distintas definiciones de inteligente, incluida la emulación del comportamiento humano y la capacidad de razonamiento lógico. En décadas recientes, sin embargo, ha surgido un consenso en torno a la idea de un agente racional que percibe y actúa para alcanzar sus objetivos al máximo. ¿Deberían preocuparnos los riesgos a largo plazo de la inteligencia artificial súper inteligente? En caso afirmativo, ¿qué podemos hacer al respecto? Aunque parte de la comunidad mayoritaria de la inteligencia artificial ignora estas preocupaciones, yo argumentaré que es necesaria una reorientación fundamental del campo. En lugar de construir sistemas que optimicen objetivos arbitrarios, necesitamos aprender a construir sistemas que nos resulten probadamente beneficiosos. Demostraré la utilidad de dotar a los sistemas de incertidumbre explícita referida respecto a los objetivos de los humanos a los que tienen que ayudar, pues para ello han sido diseñados» (Russell, 2016, pág. 179).

Ser político, en el sentido radical del término; en lo tecnológico implica un compromiso por intervenir en lo tecnológico, aunque nos exija pensar más allá del límite que hoy nos resulta pensable.

Bibliografía

Aranguren, J. L. L. (1958). *Ética* (vol. 2). Madrid: Trotta, 1994.

Aranguren, J. L. L. (1968). «La realidad constitutivamente moral del hombre: moral como estructura». En: *Ética* (págs. 56-69). Madrid: Biblioteca Nueva, 2005.

Arendt, H. (1958). *La condición humana*. Manuel Cruz (prol.). Barcelona: Paidós, 2015.

Barocas, S.; Nissenbaum, H. (2014). «Big Data's End Run around Anonymity and Consent». En: *Privacy, Big Data and the Public Good* (págs. 44-75). Nueva York: Cambridge University Press.

Bauman, Z. (2006). *Ética posmoderna*. Madrid: Siglo XXI.

Beck, U. (1992). *Risk society: Towards a New Modernity* (vol. 17). Londres: Sage.

Beyer, M. A.; Laney, D. (2012). *The Importance of «Big Data»: A Definition*. Stamford: Gartner.

Bietz, M. J.; Bloss, C. S.; Calvert, S.; Godino, J. G.; Gregory, J.; Claffey, M. P.; Patrick, K. (2016). «Opportunities and Challenges in the Use of Personal Health Data for Health Research». En: *Journal of the American Medical Informatics Association* (vol. 23 [e1]: e42-8). [Fecha de consulta: 2 de junio de 2017]. <doi: 10.1093/jamia/ocv118>

Boyd, D.; Crawford, K. (2012). «Critical Questions for Big Data - Provocations for a Cultural, Technological, and Scholarly Phenomenon». En: *Information, Communication & Society* (vol. 15, n.º 5, págs. 662-679).

Capurro, R.; Eldred, M.; Nagel, D. (2013). *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld*. Frankfurt: Ontos Verlag.

Castells, M. (2009). *Comunicación y poder*. Madrid: Alianza.

Douglas, M. (1992). *Risk and Blame: Essays in Cultural Theory*. Londres: Routledge.

Eco, U. (1973). *De la responsabilidad moral como producto tecnológico: diario mínimo*. Barcelona: Península.

Ess, C. (2006). «Ethical pluralism and global information ethics». En: *Ethics and Information Technology* (vol. 8, n.º 4, págs. 215-226).

Ess, C. (2009). «Floridi's Philosophy of Information and Information Ethics: Current Perspectives, Future Directions». En: *The Information Society* (vol. 25; n.º 3, págs. 159-168).

Etxeberría, X. (2011). «Espacios y agentes de responsabilidad pública». En: A. Hortal; X. Etxeberría (eds.). *Profesionales y vida pública* (págs. 15-35). Bilbao: Desclée de Brower.

Floridi, L. (1999). «Information Ethics: On the Philosophical Foundation of Computer Ethics». En: *Ethics and Information Technology* (vol. 1, n.º 1, págs. 33-52).

Hashem, I. A. T.; Yaqoob, I.; Anuar, N. B.; Mokhtar, S.; Gani, A.; Khan, S. U. (2015). «The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues». En: *Information Systems* (vol. 47, págs. 98-115).

Heidegger, M. (1947). *Carta sobre el humanismo*. H. Cortés; A. Leyte (trads.). Madrid: Alianza, 2000.

Johnson, D. G.; Miller, K. W. (2009). *Computer Ethics*. Nueva Jersey: Prentice Hall.

Jonas, H. (1979). *El principio de responsabilidad. Ensayo de una ética para la civilización tecnológica*. Barcelona: Herder, 1995.

Kokumai, H. (2016). «Biometrics: Great for Physical Security, Possibly a Big Mistake for Cyber Security?». En: *Biometric Technology Today* (n.º 5, págs. 7-9).

Laney, D. (2001). «3D Data Management: Controlling Data Volume, Velocity and Variety». *META Group Research Note* (n.º 6, pág. 70).

Lledó, E. (1994). *Memoria de la ética*. Madrid: Taurus, 2015.

Ortega y Gasset, J. (1939). *Meditación de la técnica y otros ensayos sobre ciencia y filosofía*. Madrid: Alianza, 1998.

Popescul, D.; Georgescu, M. (2014). «Internet of Things — Some Ethical Issues». En: *The USV Annals of Economics and Public Administration* (vol. 13, *issue* 2, n.º 18, págs. 208-214).

Russell, S. (2016). «Inteligencia artificial de beneficios probados» [artículo en línea]. En: *El próximo paso: la vida Exponencial*. BBVA-Open Mind (págs. 175-192). [Fecha de consulta: 2 de marzo de 2017]. <https://www.bbvaopenmind.com/articulo/inteligencia-artificial-de-beneficios-probados/?fullscreen=true>

Sharon, T. (2016). «The Googlization of Health Research: From Disruptive Innovation to Disruptive Ethics». En: *Personalized Medicine* (vol. 13, n.º 6, págs. 563-574).

Stahl, B. C.; Timmermans, J.; Mittelstadt, B. D. (2016). «The Ethics of Computing: A Survey of the Computing-Oriented Literature». En: *ACM Computing Surveys* (vol. 48, n.º 4).

Stylianou, A.; Talias, M. A. (2017). «Big Data in Healthcare: A Discussion on the Big Challenges». En: *Health and Technology* (vol. 7, n.º 1, págs. 97-107).

Swan, M. (2015). «Philosophy of Big Data» [informe en línea]. En: *2015 IEEE First International Conference on Big Data Computing Service and Applications* (págs. 468-477). [Fecha de consulta: 5 de septiembre de 2016]. <http://ieeexplore.ieee.org/document/7184918>

Trías, E. (2000). *Ética y condición humana*. Barcelona: Ediciones Península.

Zambrano, M. (1958). *Persona y democracia*. Madrid: Siruela, 1987.

Zubiri, X. (1944). *Naturaleza, Historia, Dios*. Madrid: Editorial Nacional.

Capítulo II

¿Qué debo hacer? ¿Lo bueno, lo justo o lo correcto? Teorías éticas y principios profesionales

1. Introducción

Mediante la ética tratamos de atender, y dar respuesta, a aquella cuestión fundamental que nos persigue, como nuestra propia sombra, a lo largo y ancho de la vida: ¿qué debo hacer?, ¿qué decisión tomar?, ¿qué criterios adoptar? Una sociedad decente, por emplear el término acuñado por Margalit,[1] o bien ordenada —justa, libre, próspera—, si seguimos a Rawls (1971), no solo requiere buenos profesionales sino, necesariamente, profesionales buenos. Esto significa que no podremos ser buenos profesionales, cumpliendo en lo técnico, si no somos, de forma simultánea, personas buenas, que cumplen con aquello *moral*. La pregunta fundamental de la ética nos confronta entonces como profesionales y como personas (Gentile, 2012). No hay posibilidad alguna de eludir esta condición inherentemente humana si no es incurriendo en el riesgo de desprendernos precisamente de una parte de

1 La idea de *sociedad decente* está basada en la conceptualización de *humillación* desarrollada por el filósofo israelí Avishai Margalit. Así, distingue entre *sociedad civilizada* como aquella en la que sus miembros no se humillan entre sí, y *sociedad decente* como aquella en la que las instituciones no humillan a las personas (Margalit, 2010).

nuestra humanidad, y ello solo si fuese posible esa consideración de la humanidad como susceptible de ser fragmentada.

Podría objetarse aquí, además, que la consideración de *bueno* despoja al término *persona* de un significado unívoco, pues podríamos encontrar tantas consideraciones de bueno como personas, como solícitamente observan nuestros estudiantes en sus primeras clases de ética. Estableceremos por ello el sentido aristotélico que adopta Howard Gardner para explicar la necesaria conexión entre los ámbitos público y privado a través del valor de virtud (ἀρετή, o *areté* griega, también traducida como 'excelencia') que atribuye al término *bueno*: el denominado *The Good Project*, trata de identificar individuos e instituciones que sean ejemplo de un *buen trabajo*, esto es, un trabajo *bien orientado*, que sea excelente en calidad, socialmente responsable y que contribuya a la realización como persona de quien lo lleva a cabo.[2]

En los cursos de ética social y profesional solemos ocuparnos de aquello que se debería hacer, olvidando con demasiada frecuencia quién debe y puede hacerlo. Este es, precisamente, el objeto de este capítulo, interpelar a aquellos quiénes deben confrontar su ser-sujetos-morales al mismo tiempo que asumen su ser-sujetos-profesionales. No se trata de un dualismo, somos personas, siempre, independientemente del momento, del día o del lugar en el que nos encontremos, y como personas somos seres inherentemente morales, como ya vimos en el anterior capítulo.

2 La influencia aristotélica mediada por la idea de eudaimonía y florecimiento humano es evidente. Véase Aristóteles (1995) y *The Good Project*: <http://www.thegoodproject.org/projects/the-good-work-project>

2. Teorías éticas. Breve introducción

Del mismo modo, en el capítulo se dejaron planteadas varias cuestiones de las que afectan a la aplicación de una ética a la actividad relacionada con la IoT y, con ella, a la obtención, gestión y utilización de BD. Entre otras, aquella que aludía a si es posible identificar lo *bueno* con lo *correcto*, a lo que podríamos añadir ahora la consideración de *justo*. En la forja de ese carácter orientado al bien que pretende la ética, es posible distinguir diferentes teorías éticas con diferentes concepciones sobre aquello que debe primar en la toma de decisiones.[3]

Los elementos que permiten distinguir estas teorías son, en primer lugar, que cada una de ellas presenta una noción de lo que es bueno o valioso, es decir, presentan su propia *teoría del valor*. Teniendo en cuenta que para que un valor sea reconocido como tal no debe referirse a una persona concreta o a un ámbito particular, sino que debe poseer la condición de poder ser aplicado de forma universal; en segundo lugar, las teorías éticas poseen aquello que se denomina una *teoría de lo correcto*, con ello tratan de establecer no tanto qué es valioso en sí, sino aquello que deberían hacer personas y/o instituciones para hacer valer o promocionar aquello que se considera un *valor*.

3 Las *teorías éticas* tratan de explicarnos desde la filosofía moral, es decir, desde la «ética pensada» (*ethica utens*), diferentes propuestas sobre cómo las personas nos enfrentamos a la toma de decisiones. La necesaria reflexión previa, la prudencia o sabiduría aristotélica, debe orientar nuestra decisión de acción, sopesando todas y cada una de estas teorías, y no adoptando de un modo acrítico alguna de ellas en exclusiva. Por esto, no deben comprenderse como un catálogo de opciones para aproximarnos a la ética, pues equivaldría a cierto relativismo moral en cuanto podrían considerarse todas y cada una de ellas con razones suficientes y plausibles a su favor.

Tradicionalmente, las teorías éticas se han agrupado en dos grandes grupos: éticas teleológicas y éticas no teleológicas. Las primeras tienen una idea preconcebida de *bien*, por ello, entienden que la elección del agente está orientada hacia el fomento del bien. Atienden, por tanto, a las consecuencias de la acción; las segundas, por su parte, sostienen que más que fomentar un tipo de valor, lo correcto es respetar dicho valor mediante el respeto a la norma que lo reconoce como tal.

Al primero de los grupos pertenece la teoría ética denominada *consecuencialismo*, de la que el *utilitarismo* es quizá su expresión más popular. De acuerdo con el *consecuencialismo*, hacer-lo-correcto implica no solo reconocer un valor sino fomentarlo mediante la acción, buscando su maximización (Pettit, 2010). Veamos un ejemplo: un dilema moral establece como valor salvar vidas, planteando dos posibilidades para la acción: una ofrece la probabilidad del cincuenta por ciento de salvar cien vidas, otra la probabilidad de salvar un total de cuarenta vidas con una certeza del ciento por cien. Según la teoría consecuencialista hacer lo correcto implica elegir aquella opción que maximiza el bien, esto es, elegir la primera de las opciones aun considerando que existe la misma probabilidad de que finalmente no se salve ninguna vida. En los laboratorios de ética se ha comprobado que las personas tendemos a considerar esta opción de forma habitual.[4] Es el argumento empleado para justificar que los coches automáticos hayan sido programados para, de acuerdo con el valor *salvar vidas*, minimizar el número de víctimas. El problema que se ha planteado es que esta mini-

4 Véase *Moral Machine Project*, Massachusetts Institute of Technology (MIT): <http://moralmachine.mit.edu>

mización implica muchas veces sacrificar al propio conductor del vehículo y sus acompañantes, algo que ha detenido bruscamente la promoción de este tipo de vehículos. Las máquinas pueden ser programadas para tomar decisiones morales, el problema deviene ahora en cómo establecer las reglas que deben considerar los programadores para orientar a la máquina hacia una decisión sea además «correcta» (Bonnefon *et al.*, 2016).

Por otro lado, la *deontología*, como representante único de las teorías no teleológicas, mantiene que toda actuación *moral* lleva implícita la aceptación y el cumplimiento de unas determinadas reglas que ponen límites tanto a la prosecución del interés, ya sea este propio o colectivo. Evitar una mala acción —mediante el cumplimiento de una norma— es la exigencia que la deontología interpone a un sujeto moral en tanto que sujeto moral. Ni las consecuencias de una acción, ni las circunstancias en las que se da dicha acción moral, afectan a la toma de decisiones. Así, lo correcto es actuar de acuerdo con la norma acordada como fundamento ético de convivencia cívica. Los códigos éticos de empresas, universidades o colegios profesionales son un ejemplo de deontología; pero también los derechos humanos son exigencias racionales no negociables, por tanto, lo correcto será atender sus requerimientos. Podría objetarse aquí, sin embargo, que la mejor forma de garantizar el respeto de los derechos humanos es fomentando su reconocimiento como valor en sí (Davis, 2010).

Así, aunque en líneas generales, el consecuencialismo considera que el *bien antecede a lo correcto*, planteando la acción moral en términos del bien como finalidad; la deontología, por su parte, plantea la acción moral en términos

de normas y deberes, por ello considera que *lo correcto antecede al bien*. El ejemplo de los derechos humanos vendría a mostrar por qué ninguna de las dos teorías debería ser considerada como infalible de modo exclusivo. Por otro lado, las denominadas éticas dialógicas, por su parte, promovidas en el siglo XX por K. O. Apel y J. Habermas, vendrían a condensar, admitiéndose la posibilidad de bastantes puntualizaciones, ambas teorías. Aunque podría considerarse, en principio, como una ética deontológica, en cuanto que no se ocupa de las consecuencias sino de entablar un diálogo entre los afectados por las normas morales para llegar a un acuerdo consensuado, es cierto que la ética discursiva reconoce explícitamente que cuando aplicamos este procedimiento racional de diálogo en casos concretos no es posible eludir la consideración de las consecuencias de tomar por correcta una norma en vez de otra (Byrum, 2017; Cortina, 2008; Habermas, 2002).

3. Un apunte sobre la condición inherentemente política de la tecnología

¿Por qué apelar a unos principios en una época en la que los datos, y más aún los BD, parecen dar por buenas décadas de positivismo y supuesta objetividad de los métodos cuantitativos? Por la sencilla razón de que los hechos a los que aluden los datos no son suficientes respecto a muchas otras variables a las que apelamos para tomar decisiones: las emociones, la cultura, la prudencia o, por supuesto, los contextos en los que operan dichos datos. Esta supuesta objetividad se

fundamenta en la pretensión última que tienen los sistemas de información (IS, por sus siglas en inglés) de eludir o evitar en su funcionamiento la intervención humana. Para alcanzar esa legítima aspiración de invulnerabilidad, y con ella de perfectibilidad, los IS deben asumir como *telos* la plena autonomía, lo que implicaría una emancipación completa de lo humano. Ello vendría a afianzar aquellos paradigmas que han asumido la validez del denominado *determinismo tecnológico* (DT). En esta hipotética situación, los IS se alzarían como sistemas neutrales, amorales y apolíticos, en los que no cabría pretensión ética alguna. Esto conduciría este trabajo, que apenas comienza, hacia un callejón sin salida.

Debemos asumir entonces, contra esta premisa, que los atributos técnicos de una tecnología deben ser analizados sociológica y éticamente, y no solo técnicamente. Esta interrelación entre ciencia, tecnología y sociedad ha conformado una corriente de pensamiento crítico que encontramos en trabajos de los años ochenta y noventa, como *Forces of Production* (Noble, 1984), *The Social Construction of Technological Systems* (Hughes *et al.* [eds.], 1987); *The Social Shaping of Technology* (MacKencie; Wajcman [eds.], 1999), y, más recientemente, *Technoscience* (Asdal *et al.* [eds.], 2007). Estos trabajos fundamentan su crítica al DT en las siguientes asunciones:

- *Las innovaciones tecnológicas, lejos de ser neutrales, siempre están orientadas a un fin político.* Esta afirmación se alza contra el argumento que considera las tecnologías en sí mismas neutrales y que lo único que puede afectar, a efectos morales, es la forma en que las sociedades deciden usarlas (Winner, 1980; 1993; 2014).

Las tecnologías pueden ser inherentemente políticas en dos sentidos: primero, porque las tecnologías pueden diseñarse, consciente o inconscientemente, para abrir ciertas opciones sociales y cerrar otras. En segundo lugar, no solo las características particulares de diseño de las tecnologías pueden ser políticas, sino que algunas tecnologías en su totalidad *son* políticas. Incluso si asumiésemos la dificultad de relacionar las tecnologías con patrones particulares de relaciones sociales, lo que sí es evidente es que algunas tecnologías son más compatibles con algunas relaciones sociales que con otras, lo que demostraría que la tecnología no es neutral, sino política (Winner, 1986).

Si reconocemos en la ciencia y la tecnología un gran poder para crear nuevos significados y nuevas entidades y, con ellos, para hacer nuevos mundos: ¿cómo obviar el posicionamiento desde el que la ciencia y las tecnologías construyen sus campos semánticos? (Haraway, 2007). Obviar lo político en la ciencia o en la tecnología implicaría entonces obviar la responsabilidad que se deriva de su desarrollo, uso o destrucción. El discurso moral y político debe ser el paradigma del discurso racional que subyace en el discurso tecnológico.

- *Las tecnologías se ven afectadas por y desde lo social, y no como un factor independiente.* Esta asunción rebate el supuesto habitual que entiende la innovación tecnológica como un factor independiente a la misma sociedad que lo genera, afectando a la sociedad *desde fuera* de la sociedad. Pretender que la tecnología cambia solo en función de sí misma, o en la estela de los avances de la ciencia, promueve una actitud pasiva de las personas ante el cambio tecnológico. Enfocando nuestras mentes hacia cómo adaptarnos al cambio tecno-

lógico, y no hacia cómo intervenir en su propia conformación. Frente a este supuesto, que obvia los mecanismos de discusión pública, toma de decisiones y acción política que los sujetos empleamos para confrontar los riesgos inherentes a todo progreso o innovación, Ulrich Beck ha desarrollado el concepto de *modernización reflexiva* a partir de *Risk Society* (Beck, 1992), y aplicándolo después a contextos como las crisis ecológicas (Beck, 1994), los roles sexuales, la familia y el amor (Beck, 1995), o las implicaciones políticas del orden impuesto por la globalización (Beck, 1997; 2000; 2005). Esta propuesta tiene implicaciones importantes, especialmente para el papel que debe representar *lo humano* en la innovación tecnológica. El progreso, mediado por la innovación tecnológica, lejos de ser un proceso que simplemente sobreviene a las sociedades, debe comprender más bien como un proceso participado y democráticamente moldeado. En este sentido, podría afirmarse que la tecnología debe progresar con lo humano, y *a pesar* de lo humano. Comprendiéndose esto humano en Beck como algo intrínsecamente político. Algo, por lo demás, ya presente en Aristóteles.

4. Principios orientadores de la acción del buen profesional

Las teorías éticas a las que aludimos se ocupan de reflexionar sobre qué es la ética o sobre cómo atendemos a la cuestión ¿qué debo hacer?, por eso se denomina a su quehacer *pensamiento moral*; las éticas aplicadas, por su parte, tratan de

ser más específicas respecto a aquello que puede orientar la toma de decisiones. La ética profesional forma parte de estas éticas aplicadas, y antes de adentrarnos en los problemas específicos que afectan a la gestión de datos masivos, abordaremos los cuatro principios profesionales que emanan de la bioética, la ética profesional con mayor trayectoria y desarrollo (Jonsen, 1998). Estos principios no deben comprenderse como recetas cerradas a casos concretos; no son normas, de hecho, sino que funcionan más bien como principios orientadores que nos deben ayudar a mantener la mente abierta respecto a cuál o cuáles de ellos deben prevalecer en una toma de decisión. Son herramientas que nos ayudan a evaluar cuánto de bueno y realizable, o de malo y evitable, apuntando a los temas, actores y metas, hay en una determinada acción posible (Hortal, 2002b, pág. 95).

En cuanto que profesionales, la finalidad de nuestra acción debe estar orientada hacia la realización de un determinado servicio u objetivo. Para evaluar si finalmente se cumple el objetivo planteado o de qué modo se cumple, se ocupa el *principio de beneficencia*. Este principio puede entenderse en términos consecuencialistas, o utilitaristas, en el que el *bien* es identificado *a priori* y la finalidad de la acción del profesional es, ante todo, lograr su maximización. Habitualmente entra en conflicto con el denominado *principio de autonomía*, de clara inspiración deontológica, y que consiste en la evaluación sobre la instrumentalización o no de las personas en el cumplimiento de dicho objetivo profesional. Considerar la autonomía, máximo exponente de la moral kantiana, implica el respeto por la dignidad individual de las personas, asumiendo que todas y cada una de las personas somos un fin en nosotras mismas y no un mero medio para alcanzar un fin,

por muy loable que este sea. Cuando los criterios anteriores entran en conflicto, lo que es más habitual de lo esperado en cuanto que nuestras actuaciones profesionales tienen como destinatarios más un colectivo social que individuos aislados, es posible recurrir al denominado *principio de justicia* que nos permitirá jerarquizar y ordenar las posibilidades de acción de acuerdo con criterios de justicia social; pero, también, el *principio de no-maleficencia* puede resultarnos especialmente útil en caso de no ser posible la aplicación de los anteriores, aplicando su máxima: *ante todo no hacer daño*.

¿Cómo deben aplicarse estos principios? Podríamos decir que de dos modos: si seguimos una perspectiva ascendente, esto es, partimos de las actuaciones y decisiones ya tomadas, o que se pretenden tomar, en una situación concreta, entonces los principios se «invocan». Por otro lado, en perspectiva descendente, la dinámica moral parte de unos principios generales con la intención de llegar a otros más específicos que nos permitan tomar decisiones ajustadas a un determinado contexto, en este caso, mantiene Hortal, los principios se aplican (Hortal, 2002a). En ambos casos, precisamos los principios para ayudarnos bien a validar una decisión, bien para tomar una decisión a la luz de los principios. Son, además, perspectivas que, lejos de excluirse, se complementan.

4.1. Principio de beneficencia

El principio de beneficencia alude, en primer lugar, a la exigencia básica de «hacer bien» nuestro trabajo profesional, de forma competente, eficiente, correcta, ordenada y responsable, de acuerdo con los estándares de excelencia que el

colectivo de profesionales al que pertenecemos ha establecido; pero, además, se refiere a «hacer el bien», promover el bien mediante la realización de dicha actividad.[5] Es por esto por lo que es importante saber identificar aquellos valores y/o bienes que consideramos *deben ser promovidos* con nuestra acción profesional, ya sea como individuos o como corporaciones. Valgan como ejemplos: la veracidad de los contenidos de un medio, salvaguardar la intimidad y privacidad de las personas que hacen uso de nuestros servicios o aplicaciones, salvar vidas, limitar la emisión de gases contaminantes, preservar los recursos naturales, ralentizar el cambio climático, etc.

De forma simultánea deberán considerarse las consecuencias de dicha acción, es decir, los beneficios y los daños que puedan generarse, pues, aun con una finalidad orientada al bien, los daños a terceros, o bien a la autonomía de los destinatarios de nuestra acción. Así, aunque este principio profesional ha sido interpretado muchas veces como puramente utilitarista, es decir, maximizar el bien para el mayor número, debe ser comprendido en los términos que quedaron expuestos en el Informe Belmont (1979): «Beneficencia se entiende como una combinación complementaria de dos reglas básicas: 1) no causar ningún daño; y 2) maximizar los posibles beneficios, disminuyendo los posibles daños».[6]

5 La Ética a Nicómaco comienza con toda una declaración de principios sobre aquello que impulsa la acción humana: «Parece que todo arte y toda investigación, e igualmente toda actividad y elección, tienden a un determinado bien; de ahí que algunos hayan manifestado con razón que el bien es aquello a lo que todas las cosas aspiran» (Aristóteles, 1995, libro I, 1094a).

6 El Informe Belmont fue redactado para la protección de las personas, sujetos objeto de investigaciones biomédicas. Sus antecedentes son la Declaración de Helsinki (1964) y el Código Nuremberg (1949). En él se formularon por primera vez, y de forma conjunta, los *principios* a los que aludimos aquí y que han sido asu-

Si recordamos la definición de ética, vista en el primer capítulo, como conformación de un carácter mediante el hábito y la costumbre, podremos comprender el sentido que Hegel le da al término *Sittlichkeit* o eticidad: «cultura moral sedimentada en las costumbres e instituciones», y con ella el sentido de este principio que implica necesariamente que nos hacemos buenos (personas y profesionales) haciendo el bien (haciendo nuestro trabajo tal y como ha sido establecido, pero también para el bien de aquellos a quienes se dirige nuestra actividad).

4.2. Principio de autonomía

La autonomía forma parte del sistema de valores heredados de la Ilustración —junto a la dignidad y la solidaridad— y es considerada uno de los principios básicos para enfrentar la toma de decisiones en asuntos especialmente controvertidos relacionados con el inicio o el final de la vida, es decir, aquellos de los que se ocupa la bioética. Actualmente, la autonomía es considerada también un principio profesional ineludible para confrontar decisiones en toda ética aplicada a las profesiones.

El *sapere aude* kantiano queda establecido como lema de la Ilustración y ello es lo que nos permite considerar la autono-

midos por el resto de las éticas aplicadas a las diferentes actividades profesionales. *Cfr.* (1979). *The Belmont Report: Ethical Guidelines for the Protection of Human Subjects of Research*, Washington: Department of Health, Education, and Welfare: <http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report>. Existen diferentes versiones accesibles en castellano, entre otras, la del *Observatori de Bioética y Dret* de la Universidad de Barcelona: <http://www.bioeticayderecho.ub.edu/archivos/norm/InformeBelmont.pdf>

mía como el valor que guiará el cambio de época que emerge tras las revoluciones americana y francesa. ¡Atrévete a pensar por ti mismo!, nos exhorta Kant, estableciendo con ello los cimientos de la estrecha urdimbre que conforman libertad y responsabilidad para la idea de ciudadanía que viene (Kant, 2007). La consideración de la dignidad de la persona, el respeto a la autonomía de su voluntad y a su intimidad, entronca con los derechos garantizados en los artículos 10 y 18 de la Constitución Española de 1978. La relación entre esta autonomía que realiza al ser humano como tal y la moral, mediada por la responsabilidad, es establecida por Camps del siguiente modo:

La autonomía no es solo ese espacio en el que somos libres para decidir porque ninguna prohibición se nos cruza en el camino, sino que es la facultad por la que nos preguntamos y damos respuesta a la pregunta fundamental: ¿qué debo hacer? Dicho de otra forma, en la medida en la que es capaz de razonar, al ser autónomo no le está permitido éticamente hacer lo que le parezca, sino que debe hacer lo que le propone la ley moral […] La autonomía moral no consiste solo en la libertad de elegir, en la ausencia de restricciones, sino en la capacidad para elegir bien […] El ser autónomo, el ser humano, es, al mismo tiempo, moral, puesto que, siempre que piense desde la razón y no desde el sentimiento, las normas o leyes que se dará a sí mismo serán leyes morales. Cuando digo: «debo hacer esto, aunque no me apetezca hacerlo», estoy hablando desde la razón y no desde el sentimiento o el deseo, me estoy imponiendo una manera de actuar que tiene una explicación o una justificación finalmente moral. Kant concibe al individuo como una voluntad escindida en dos partes que suelen ser antagónicas: la razón y la sensibilidad.

Lo que la razón dicta como correcto y justo no suele ser lo que la sensibilidad apetece. La tarea moral consiste en lograr que se imponga la razón sobre la sensibilidad (Camps, 2005, págs. 110-114).

La autonomía que debemos considerar aquí, en tanto que principio profesional, es la autonomía de nuestros clientes, pacientes o destinatarios finales de nuestro quehacer profesional. Una autonomía que implica la libertad y autodeterminación de una persona para tomar decisiones por sí misma en aquellos asuntos que afecten a su propia vida, a su propio cuerpo o mente, con la limitación expresa que supone reconocer, a su vez, a los demás como sujetos autónomos, con libertad y derechos. Facilitar información precisa y clara sobre el alcance de la investigación o de la actividad concreta, es lo que denominamos *consentimiento informado* y tiene la función de materializar el reconocimiento de dicho principio por parte de los profesionales. Podríamos establecer tres momentos en la dinámica de toda acción autónoma: i) el sujeto debe tener capacidad racional para elegir críticamente entre diferentes cursos de acción; ii) debe poseer habilidades, mentales y/o físicas, para alcanzar los fines «elegidos»; y, finalmente, iv) debe observar cierto sentido de la responsabilidad tanto en el momento de la deliberación (*ex ante*) como tras la ejecución de la acción elegida (*ex post*) (Ricoeur, 1995).

La consideración de la autonomía es, finalmente, lo que establece los límites a una aplicación «paternalista» del principio de beneficencia. Esta asimetría entre cliente/ paciente y profesional, derivada de la posición de poder y relativa dominación de un determinado campo profesional, por formación, acreditación y, en su caso, reputación, puede llegar a ser abusiva cuando un profesional toma decisiones que afec-

tan a su cliente/ paciente sin atender sus propios criterios e, incluso, sin su consentimiento. En el área de la gestión masiva de datos, podríamos decir que tomar el principio de autonomía «en serio» implica que las personas deben poder tomar sus propias decisiones en aquellas cuestiones que afecten a su propia intimidad, privacidad, utilización y difusión de datos que ellos mismos generan, aunque no sean de su propiedad (Grady *et al.*, 2017; Pascalev, 2017). La autonomía ha sido considerada por muchos como un espejismo imposible de alcanzar ante la evidencia ineludible de un determinismo social y económico que actualmente es, además, tecnológico, como vimos antes. Y ello, especialmente, si se considera la autonomía del sujeto, sustentada en su capacidad de raciocinio, como única fuente de valor para resolver dilemas morales o tomar decisiones. El determinismo tecnológico afecta a nuestra autonomía moral a través de la introducción de algoritmos que deciden por nosotros, o incluso por las propias empresas como Google o Facebook, qué contenido es adecuado y cuál no. De hecho, depositar en sus algoritmos la responsabilidad de algunos sonados errores cometidos tanto por Google como por Facebook les permite zafarse, como empresas, de algunas cuestiones éticas nada irrelevantes relacionadas con la autonomía de sus usuarios que, como humanos que son, quieren realizarse como tales tomando sus propias decisiones sobre aquello que afecta a sus propias vidas (Morozov, 2015).

4.3. Principio de no-maleficencia

La formulación latina de este precepto reza *primum non nocere*, esto es, ante todo, no hacer daño. Se trata de un principio que

aunque ha visto modificado su sentido a lo largo de la historia, tal y como mostró Diego Gracia en su discurso de entrada en la Real Academia Nacional de Medicina en 1990, puede y debe considerarse el principio rector de toda la ética médica, desde los hipocráticos[7] hasta la actual bioética (Gracia, 1990).

Así, aunque en su formulación griega la sentencia manda al médico «favorecer, o al menos no perjudicar», distingue claramente entre las dos acciones. La primera, favorecer, correspondería al principio de beneficencia, mientras que la segunda al principio de no-maleficencia que nos ocupa. Gracia (1990) mantiene en su discurso que la expresión latina, tal y como nos ha llegado, procede muy probablemente de Escribonio Largo, un farmacólogo romano que vivió en el siglo I. El *primum non nocere*, al dejar atrás el mero *favorecer*, sumaría a su condición de precepto puramente técnico su interpretación como precepto moral. Lo que vendría a significar que a un médico o farmacólogo no solo se le exige ser un virtuoso técnicamente, sino además y simultáneamente, un farmacólogo virtuoso. La aplicación técnica de este principio implica una «minimización» de los daños, pero esta no es sino un mandato moral que exige preceptivamente *no hacer daño*. Aunque en realidad no sería hasta el siglo XVII, con la formulación de los primeros derechos humanos: Locke (1632-1704) consideró que todo hombre tiene desde el principio derecho a la vida, a la libertad de conciencia y a la propiedad, que pueda hablarse de una ética racional auténticamente deontológica. Una ética

7 El denominado *Corpus hippocraticum* está conformado por más de setenta libros atribuidos a Hipócrates de Cos, médico griego que vivió entre el 460 a. C. y el 370 a. C. Aunque los expertos coinciden en atribuir a este autor únicamente cuatro de estas obras: *Epidemias I, Epidemias III*, *Pronóstico* y *Sobre la dieta en las enfermedades agudas*. *Cfr.* (Hipócrates de Cos, 1985).

que considera que estos absolutos le son dados u otorgados al ser humano por la naturaleza, siendo por tanto anteriores a cualquier legislación o contrato social.

Frente al liberalismo clásico, del que son representantes no solo Locke sino también Adam Smith y John Stuart Mill, el liberalismo del siglo XX introduce la justicia como catalizador para abordar la problemática que se da en la periferia de estos principios (Sen, 2012). Frente al utilitarismo que representa el estado benefactor que pretende la máxima felicidad para la mayor parte de sus ciudadanos, aun a riesgo de atropellar los derechos de alguno, Nozick introduce el término *side-constrainsts* mediante la formulación «los derechos de los otros determinan los límites de tus propias acciones». Esto es, los derechos no son algo que pueda manipularse con el fin de maximizar los objetivos, sino que funcionan como límites. La no-maleficencia implicará no superar dichos límites. Para Nozick, la función primera e ineludible del estado será velar por salvaguardar los derechos individuales de sus ciudadanos, un mandato deontológico que está por encima de sí mismo: el principio que debe aplicar entonces es el de no-maleficencia y no el de beneficencia (Nozick, 1988).

Lo que viene a mostrar Gracia es que mientras el principio de beneficencia es esencialmente consecuencialista, pues busca maximizar aquello que un profesional comprende como «bien», admitiéndose cierto «mal» si es con el objeto de lograr un bien mayor. Cuando el nivel de ese mal admitido queda establecido por el profesional, ignorando la autonomía de la persona hacia la que se dirige la acción, hablamos de paternalismo; el principio de no-maleficencia es esencialmente deontológico en cuanto que alude a principios universales que han de comprenderse como ante-

riores a cualquier consideración particular. El principio de no-maleficencia es considerado entonces como el principio por antonomasia, el que debe orientar primariamente en la toma de decisiones cuando los demás principios entran en conflicto.[8]

4.4. Principio de justicia

La idea de justicia está ligada al principio de no-maleficencia tanto como el de beneficencia lo está a la idea de moral: podemos elegir hacer el bien, nuestra capacidad de distinguir el bien del mal, y de elegir, nos hace intrínsecamente morales, pero no podemos sentirnos libres para hacer el mal (a otros) en tanto que existe un mandato que está por encima de nuestra libertad y autonomía que nos lo impide.

8 El conflicto sobre vacunar o no vacunar a los niños es un ejemplo que ilustra perfectamente el dilema entre atender un «bien» para la mayoría, lo que puede ser erradicar una enfermedad infecciosa dentro de una población mediante una vacunación masiva, como ha ocurrido con enfermedades como la difteria, o considerar la autonomía del paciente, en este caso una autonomía diferida a los padres o tutores del menor, que pueden optar por no vacunar a su vástago por no querer asumir los riesgos de los efectos secundarios que la vacunación implica en muchos casos. La Ley 41/2002, del 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, reconoce el derecho del paciente a no acatar obligatoriamente las recomendaciones médicas, con lo que resuelve el conflicto entre el principio de beneficencia y el de autonomía a favor de este último. El fallecimiento de un niño de seis años tras contraer la difteria por no estar vacunado generó una polémica en la que tuvo que intervenir el Comité Nacional de Bioética, considerando en qué casos el principio de no-maleficencia, no favorecer la propagación de la enfermedad, debería primar sobre el de autonomía. *Cfr.* «El Comité de Bioética recomienda ampliar la obligación de vacunar». *El País*, 9 de febrero de 2016: <http://politica.elpais.com/politica/2016/02/09/actualidad/1455036981_427745.html>

Esta obligación puede ser *perfecta*, la que nos liga a los derechos humanos negativos, derechos civiles y políticos, o *imperfecta*, que es la que nos liga con los derechos humanos positivos, es decir, los derechos económicos, sociales y culturales. En la teoría de la justicia que plantea Rawls coexisten dos principios: aquel que considera el mayor sistema de libertad para todos y el de igualdad de oportunidades, que Rawls denomina *justicia como equidad*. Podría incorporarse uno más, el denominado principio de la diferencia, que establece que las desigualdades solo son justificables si redundan en beneficio de todos, pero muy especialmente de los más desfavorecidos, de las minorías o de los excluidos (Rawls, 1971). La justicia, y aquí volvemos a Gracia (1990), es a la no-maleficencia como la autonomía es a la beneficencia:

> «No hay beneficencia sin autonomía, ni no-maleficencia sin justicia […] La no-maleficencia no puede ni debe definirse desde la beneficencia, como se hizo clásicamente, pero tampoco desde la autonomía, al modo del liberalismo doctrinario, sino desde la justicia» (Gracia, 1990, pág. 74).

Así, si la aportación fundamental de la ética de la modernidad fue la idea de autonomía, es decir, el derecho humano a la libertad moral, hoy se podría decir que la aportación fundamental de la ética del siglo XX es que el único principio que goza de la consideración de absoluto es el de no-maleficencia mediado por el de justicia.

Bibliografía

Asdal, K.; Brenna, B.; Moser, I. (eds.) (2007). *Technoscience. The Politics of Interventions*. Oslo: Oslo Academic Press.

Aristóteles (1995). *Ética nicomáquea*. J. Pallí Bonet (trad.). Madrid: Gredos.

Beck, U. (1992). *Risk Society: Towards a New Modernity. Volume 17*. Londres: Sage.

Beck, U. (1994). *Ecological Politics in the Age of Risk*. Cambridge: Polity Press.

Beck, U. (1995). *The Normal Chaos of Love*. Cambridge: Polity Press.

Beck, U. (1997). *The Reinvention of Politics. Rethinking Modernity in the Global Social order*. Cambridge: Polity Press.

Beck, U. (2000). *What is Globalization?* Cambridge: Polity Press.

Beck, U. (2005). *Power in the Global Age*. Cambridge: Polity Press.

Bijker, W.; Pinch, T.; Hughes, T. P. (eds.) (1987). *The Social Construction of Technological Systems: New Approaches in the Sociology and History of Technology*. Cambridge: MIT Press.

Bonnefon, J. F.; Shariff, A.; Rahwan, I. (2016). «The Social Dilemma of Autonomous Vehicles». En: *Science* (vol. 352, n.º 6.293, págs. 1.573-1.576).

Byrum, K. (2017). «The European Right to be Forgotten: A Challenge to the United States Constitution's First Amendment and to Professional Public Relations Ethics». En: *Public Relations Review* (vol. 43, n.º 1, págs. 102-111).

Camps, V. (2005). *La voluntad de vivir*. Barcelona: Ariel.

Cortina, A. (2008). «La ética discursiva». En: V. Camps (ed.). *Historia de la ética* (vol. 3, págs. 532-576). Barcelona: Crítica.

Davis, N. A. (2010). «La deontología contemporánea». En: P. Singer (ed.). *Compendio de Ética* (págs. 291-307). Madrid: Alianza.

Gentile, M. C. (2012). *Dar voz a los valores*. J. M. Lozano (prol.). Barcelona: Proteus.

Gracia, D. (1990). *Primum non nocere: El principio de no-maleficencia como fundamento de la ética médica. Discurso para la recepción pública en la Real Academia Nacional de Medicina de Diego Gracia Guillén; y contestación de Pedro Laín Entralgo* [publicación en línea]. Madrid: Anzos. [Fecha de consulta: 5 de noviembre de 2016]. <http://bibliotecavirtual.ranm.es/ranm/es/consulta/registro.cmd?id=617>

Grady, C.; Cummings, S. R.; Rowbotham, M. C.; McConnell, M. V.; Ashley, E. A.; Kang, G. (2017). «The Changing Face of Informed Consent». En: *New England Journal of Medicine* (vol. 376, n.º 9, págs. 856-867).

Habermas, J. (2002). *Conciencia moral y acción comunicativa*. Barcelona: Península.

Haraway, D. (2007). «Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective». En: K. Asdal; B. Brenna; I. Moser (eds.). *Technoscience. The Politics of Interventions* (págs. 21-46). Oslo: Oslo Academic Press.

Hipócrates de Cos (1985). *Tratados Hipocráticos*. Carlos García Gual (ed.). Madrid: Gredos.

Hortal, A. (2002a). «Ética aplicada y conocimiento moral». En: Domingo García Marzá (comp.). *El estatuto de la ética aplicada*. Castellón: Universidad Jaume I.

Hortal, A. (2002b). *Ética general de las profesiones*. Bilbao: Desclée de Brower.

Kant, I. (2007). «Contestación a la pregunta: ¿Qué es la Ilustración?». En: R. R. Aramayo (ed., trad., prol.). *¿Qué es la Ilustración? y otros escritos de ética, política y filosofía de la historia* (págs. 83-93). Madrid: Alianza.

MacKenzie, D.; Wajcman, J. (1999). *The Social Shaping of Technology*. D. MacKenzie; J. Wajcman (eds.). Buckingham: Open University Press.

Margalit, A. (2010). *La sociedad decente*. Barcelona: Paidós.

Morozov, E. (2015). «Los peligros de la mediación algorítmica». En: *La locura del solucionismo tecnológico* (págs. 165-206). Madrid: Katz Editores.

Noble, D. (1984). *Forces of Production: A Social History of Industrial Production*. Nueva York: Knopf.

Nozick, R. (1988). *Anarquía, Estado y utopía*. México: Fondo de Cultura Económica.

Pascalev, M. (2017). «Privacy Exchanges: Restoring Consent in Privacy Self-Management». En: *Ethics and Information Technology* (vol. 19, n.º 1, págs. 39-48).

Pettit, P. (2010). «El consecuencialismo». En: P. Singer (ed.). *Compendio de Ética* (págs. 323-346). Madrid: Alianza.

Rawls, J. (1971). *A Theory of Justice*. Massachussets: Harvard University Press.

Ricoeur, P. (1995). *Le juste*. París: Esprit.

Sen, A. (2012). *La idea de la justicia*. Madrid: Taurus.

Winner, L. (1980). «Do artifacts have politics?». En: *Daedalus* (vol. 109, n.º 1, págs. 121-136).

Winner, L. (1986). *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: The University of Chicago Press.

Winner, L. (1993). «Upon Opening the Black Box and Finding it Empty: Social Constructivism and the Philosophy of Technology». En: *Science, Technology & Human Values* (vol. 18, n.º 3, págs. 362-378).

Winner, L. (2014). «Technologies as Forms of Life». En: R. L. Sandler (ed.). *Ethics and Emerging Technologies* (págs. 48-60). Londres: Palgrave Macmillan UK.

Capítulo III

Problemas éticos fundamentales que afectan a la gestión de *big data*

Nadie será objeto de injerencias arbitrarias en su vida privada, en su familia, en su domicilio o en su correspondencia, ni de ataques contra su honor y reputación. Toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques.

Artículo 12 de la Declaración Universal de los Derechos Humanos (1948)

1. Introducción

Es habitual aludir a la neutralidad de los datos para justificar lo innecesario de la ética en lo que se denominan ciencias puramente empíricas. Después de la lectura de los dos primeros capítulos, esperamos que esta afirmación no les deje indiferentes. Los datos tienen una fuente, son obtenidos bien a partir de personas o de las actividades que realizan dichas personas, con unos determinados métodos y con una o varias finalidades. Analizar este proceso nos llevará inmediatamente a plantearnos distintas cuestiones que tendrán, ineludiblemente, implicaciones éticas.

En los albores del periodismo digital, Richard Mason (1986) ya estableció cuáles eran los temas éticos esenciales que emergían de la interacción entre tecnologías de la información y derechos humanos. Entre ellos, se encontraban la intimidad, la exactitud, la propiedad intelectual y la accesibi-

lidad.[1] En plena eclosión de la IoT, estos problemas podrían ser reformulados en identidad, privacidad, propiedad y reputación. De hecho, son considerados la estructura esencial a partir de la cual construir una ética aplicada a los BD (Davis; Patterson, 2012). El tamaño y omnipresencia de estas grandes colecciones de datos[2] están forzando nuevas cuestiones relacionadas con nuestra identidad, los cambios en nuestra valoración de la privacidad y la intimidad, el significado real de poseer/controlar datos propios y ajenos, y sobre cómo gestionamos nuestra reputación, tanto en modo *online* como *offline*, una vez asumido que nuestros datos *online* no solo la afectan sino que de hecho la moldean y conforman cada día. Existe, por tanto, una necesidad académica, profesional y ciudadana de confrontar los problemas que surgen en este espacio de intersección, pues es en este espacio donde se están conformando las sociedades del siglo XXI (Taylor, 2016).

2. Identidad

La proposición ética precisa un sujeto moral que se haga cargo de la realidad mediante una respuesta responsable. Ese

1 Mason utilizaba el acrónimo PAPA para referirse a estos cuatro aspectos éticos: *Privacy*, *Accuracy*, *Property* y *Accessibility*.

2 Entendemos BD como una constelación de fenómenos relacionados con la producción, consumo, recopilación y análisis de grandes colecciones de datos producidos por una gran variedad de fuentes, en gran número de formatos, en unas cantidades sin precedentes y que fluyen en red a gran velocidad, y cuya finalidad última es ser convenientemente analizados con objeto de extraer valor para empresas, gobiernos e instituciones públicas y privadas (Bello-Orgaz *et al*., 2016).

sujeto moral, humano, debe asumir la doble máxima del oráculo de Delfos: «nada sin medida» y «conócete a ti mismo»; ancestrales comentarios de la proposición ética que nos exigen «armonizar la conducta con la naturaleza y carácter de la *humana conditio*», esto es, aquella que nos permite asumir nuestra humanidad (Trías, 2000, pág. 82).

La complejidad de este sujeto moral, fragmentado en tres, en el espacio del límite que representa la trascendencia de lo ético: un sujeto I que pronuncia el imperativo ético, una voz de la conciencia, que dicta «obra de tal manera que llegues a ser lo que eres, límite y frontera del mundo»; un sujeto II que escucha esa frase, aun antes de decidirse a actuar y considera tan solo las distintas opciones posibles que deberían conformar una respuesta; y, finalmente, el sujeto III, que argumenta, o justifica, diría Aranguren, la respuesta elegida mediante la ejecución de la acción, ya sea en armonía o en discordia con aquello que el sujeto I le propuso (Trías, 2000, págs. 86-94).

Hemos retomado aquí lo que se denomina *dinámica de la acción moral* para considerar ahora quiénes pueden adoptar ese rol de sujeto moral en el sistema en el que intervienen los BD. Tenemos en primer lugar al usuario que interactúa con cualquier dispositivo electrónico en red. El usuario es, simultáneamente, productor, pues los datos afectados por la ética que abordamos aquí son, esencialmente, datos que proceden de personas, y consumidor de datos ya procesados y orientados hacia un fin concreto: lo llamaremos aquí *prosumers*.[3] ¿Qué

3 Aunque su origen pueda ubicarse en los años setenta del pasado siglo, el término *prosumer* comenzó a utilizarse en los círculos tecnológicos en los primeros años del siglo XXI para llamar la atención sobre el hecho de que los consumidores de los servicios de BD son, además, los productores de los datos que conforman los propios repositorios de datos masivos.

relación existe entre la identidad *online* y la identidad *offline* de este usuario? ¿Es consciente de cómo su identidad se transforma, moldea y adapta en su interacción con los dispositivos conectados con los que accede a la red?

El juez Gary Brown de la ciudad de Nueva York consideró en una sentencia que una dirección de IP no es suficiente evidencia para identificar a infractores de delitos relacionados con los derechos de autor (Davis; Patterson, 2012, pág. 3). Al considerar que una persona no es una dirección de IP, entonces, ¿podrían considerarse los datos generados por una específica dirección de IP legalmente asociados con un sujeto único, con un individuo? Las implicaciones de esta sentencia van más allá de aquellos que cometen infracciones relacionadas con los derechos de autor; supone un primer desvanecimiento del sujeto y con él la posibilidad de atender las consecuencias de la acción, esto es, la responsabilidad, que se desdibuja gracias a una dirección de IP que no se identifica con el sujeto, porque no es idéntica a él. ¿Cómo podría serlo?

Pero hay otras identidades posibles como *prosumers*: cuando interactuamos en Facebook o Twitter estamos trazando una *lifestream* perdurable en el tiempo no tanto como nosotros consideremos sino como consideren los gestores de esas redes sociales.[4] Esto tiene además relación con la propiedad, pero también con la reputación y, por supuesto, con la privacidad. Los datos personales que conforman esa *lifestream* son

4 La Biblioteca del Congreso de los Estados Unidos está archivando todos los tuits producidos desde 2006 en la red social Twitter. Por otro lado, Facebook ha reconocido tácitamente que cuando alguien decide darse de baja borrando su propia cuenta no borra simultáneamente los datos asociados a dicha cuenta, que quedan almacenados y registrados con la identidad de quien los generó.

todos los datos generados en el curso de la vida de una persona interactuando con un dispositivo aquello que algunos han denominado el *yo cuantificado* (Morozov, 2015). Gordon Bell, ingeniero de Microsoft, comenzó a registrar sistemáticamente en 1990 todas las acciones susceptibles de ser cuantificadas de su día a día:

> «(He registrado) toda una vida de notas periodísticas, libros, discos compactos, cartas, memos, artículos científicos, fotografías, presentaciones, películas caseras, conferencias grabadas [...], grabaciones de conversaciones telefónicas, transcripciones de mensajería instantánea, años de correos electrónicos, búsquedas en internet y actividades diarias» (Bell; Gemmell, 2010).

A esto hay que añadir las imágenes tomadas cada veinte segundos por un dispositivo, una *SenseCam*, que Bell fijaba al cuello de su camisa con la que habrá generado casi tres mil fotografías al día. ¿Podemos considerar esto que Bell denominó *lifelogging* un antecedente del *yo cuantificado* o, más bien, debemos ver en Bell un ideólogo que ha buscado una solución tecnológica a una opción personal que ha devenido universal?

Hay algo más, la identidad que surge a partir de esta cuantificación constante, ¿es necesariamente prismática o, por el contrario, solo si es única podremos considerarnos personas íntegras? Estas dos visiones diametralmente opuestas son las que mantienen, respectivamente, Christopher Poole y Mark Zuckerberg.[5] Aunque resulte paradójico, ambas interpreta-

5 Christopher Poole es el fundador de 4Chan y Canvas. En febrero de 2016 fue contratado por Google. Ha defendido la necesidad de potenciar el anonimato en la red, lo que ha generado discusiones muy controvertidas. Sobre su propuesta con relación al concepto de *identidad poliédrica*, véase «You Are Not Your Name and Photo, a Call to Re-imagine Identity», Tim Carmody, *Wired*, 20 de noviembre

ciones comprenden las transformaciones que el fenómeno BD está aportando al concepto de identidad: en tanto que BD habilita a otros a localizar, recopilar y resumir diferentes facetas de nuestra identidad —sin nuestra participación, autorización o acuerdo explícito—, este fenómeno está haciendo evolucionar el concepto de identidad hasta el punto que necesariamente debemos considerar los cambios que esto implica respecto a nuestra relación ética con el concepto que el término representa. Cuanto más alineadas estén nuestras acciones con la evolución y expansión de nuestra identidad, más explícita y plenamente podremos entender los valores con los que nos identificamos y nos permiten, asimismo, tomar decisiones en un sentido o en otro. En nuestra interacción con la tecnología, como en cualquier otra forma de acción humana, la cuestión no es solo qué uso hacemos de ella sino, esencialmente, en qué tipo de persona nos transformamos cuando estamos utilizando esta tecnología. Efectivamente, en la red ya no somos lo que nosotros pretendemos ser, nuestra identidad, es una identidad poliédrica de la que somos solo en parte responsables, el alcance de la función que desempeña la intimidad/privacidad de nuestra identidad entra aquí en juego.

Nos hemos referido aquí hasta ahora al riesgo en el que incurren los individuos, sin embargo, usuarios *comsumers*

de 2010: <https://www.wired.com/2011/10/you-are-not-your-name-and-photo-a-call-to-re-imagine-identity>. Mark Zuckerberg es el fundador de Facebook. A pesar del funcionamiento de la red social respecto a la identidad de sus usuarios, Zuckerberg ha considerado habitualmente que la integridad de las personas implica el mantenimiento en la red de una identidad única, lo que entra en conflicto con la posición de Poole. Véase «Facebook, Foe of Anonymity, is Forced to Explain a Secret», Miguel Helft, *The New York Times*, 13 de mayo de 2011: <http://www.nytimes.com/2011/05/14/technology/14facebook.html>

pueden ser considerados también hospitales, instituciones educativas o de gobierno, o las propias empresas. Todas ellas incurren en riesgo de perder el control, y por tanto de producir daños, tanto sobre los datos recogidos, de sus pacientes, estudiantes, ciudadanos o clientes, como de los datos ya gestionados con una intención concreta.[6] La identidad de estos *comsumers* está íntimamente relacionada con la cultura de su organización y ligada inevitablemente al concepto de reputación. La dimensión, el tipo o el impacto de estos riesgos son difíciles de establecer *a priori*. ¿Cuáles son los riesgos potenciales si las consecuencias de una acción no son diagnosticadas ni atendidas? ¿Cómo podría una organización argumentar racionalmente sobre la justificación para correlacionar la información sobre el historial sanitario de una persona con información acerca de sus búsquedas en línea? ¿De qué modo afecta el resultado de esta correlación a nuestra identidad?

6 Proponemos aquí un nuevo término, que es ocasionalmente utilizado en *marketing* para caracterizar a un tipo de consumidor al que nosotros hemos denominado en este trabajo *prosumer*. Los *comsumers* son ahora entendidos, en este caso, como aquellos proveedores de servicios (Movistar, Orange, Verizon, etc.), instituciones públicas sanitarias, educativas o de gestión ciudadana que utilizan medios digitales para facilitar el servicio al que están destinadas, un gestor de dispositivos en línea, como Apple, Android, etc., o cualquier otra empresa o corporación privada o pública que comercializa o utiliza los datos ya analizados, ya sea con fines lucrativos, de investigación o de gestión pública, pero que, a su vez, y de forma simultánea, es un consumidor de datos producidos por los mismos usuarios (*prosumers*) a los que da servicio.

3. Vulnerabilidades visibles e invisibles de la privacidad en el contexto de *big data*

El dualismo que subyace en toda discusión sobre privacidad es aquel que confronta, de un lado, la demanda de seguridad y, con ella, la necesidad de vigilancia; y, de otro, los efectos que dicha vigilancia tienen sobre la libertad individual y colectiva, lo que implica una ineludible consideración de los horizontes y los límites de dicha vigilancia. Así, mientras en el primer caso la vigilancia es la mejor forma de procurar un espacio de seguridad mínima, sin la cual tampoco sería posible asegurar la libertad individual; en el segundo, el «vigilante» se rebela con un poder que amenaza los derechos civiles del mismo sujeto que trata de proteger. La cuestión de la privacidad quedaría entonces atrapada en el oxímoron *vigilar para la liberar* que nos lleva de una exigencia de libertad individual mediada por la legítima demanda de protección y, simultáneamente, a una pérdida de libertad y autonomía mediada por la utilización de medios para la vigilancia que, en muchos casos, excede la mera «observación», en cuanto que dichos medios conforman un sistema de información que tiene entre sus pretensiones *controlar* y *monitorizar*. En palabras de Zygmunt Bauman, «la promoción de la seguridad requiere siempre el sacrificio de la libertad, aun cuanto esta solo puede ser ampliada a costa de mayor seguridad. Es más, seguridad sin libertad equivale a esclavitud […] y libertad sin seguridad equivale a estar perdido y abandonado» (Bauman, 2003, pág. 24).

Estos planteamientos se encuentran ya en el *Leviatán* de Hobbes (1651), por lo que su planteamiento está muy lejos de una pretensión de novedad. Los que sí han cambiado, muy especialmente a partir de los años noventa, son los medios

de los que se sirve el poder para ofrecer seguridad mediante el ejercicio de la vigilancia y, especialmente, la naturaleza de los motivos por los que la seguridad de los estados está ahora más amenazada que nunca (Kapferer, 2004). El estudio de este dualismo seguridad (vigilancia) y privacidad (derechos civiles) puede ser abordado atendiendo a dos hitos fundamentales: i) los atentados terroristas del 11 de septiembre de 2001 en Nueva York y Washington y ii) la revelación de pruebas que verificaron el espionaje masivo que habría estado llevando a cabo el gobierno de los Estados Unidos sobre su propia población realizada por Edward Snowden, en 2013.[7]

En los trabajos previos al 11S se plantearon ya amplios campos de discusión sobre los cambios sociales, políticos y culturales que implicaría el uso de nuevos instrumentos tecnológicos de recopilación, almacenamiento, interpretación y posterior uso de datos personales asociados a la vigilancia (Lyon, 1994; Marx, 1988; McCahill, 1998; Rule, 1973; Westin, 1967). Todos ellos son considerados trabajos visionarios, pues «anticiparon el papel dominante que los sofisticados sistemas tecnológicos asumirían en la vida cotidiana de la ciudadanía en las sociedades occidentales contemporáneas» (Frois, 2011, pág. 13). Tras el hito del 11S, los sistemas de vigilancia se multiplicaron haciéndose más sofisticados y, con ello, con mayor capacidad de penetración en las capas más internas de la intimidad y la privacidad de las personas. Nos referimos fundamentalmente a: i) la instalación de cámaras

7 Edward Snowden, técnico informático que trabajó para la CIA y la NSA, agencias de información del gobierno de los Estados Unidos, reveló a los periódicos *The Guardian* y *The Washington Post*, en junio de 2013, los programas de vigilancia masiva que estaban siendo ejecutados ilegalmente por estas agencias.

de video vigilancia (CCT, por sus siglas en inglés: *closed circuit television*) tanto en el espacio público abierto de las ciudades, como hospitales, centros comerciales, estadios deportivos, etc., que si bien comenzó en los años noventa (Norris; Armstrong, 1999), su uso generalizado se extiende a partir de las exigencias de seguridad en aquellos lugares sede de acontecimientos deportivos multitudinarios como las Olimpiadas de Atenas de 2004 (Samatas, 2004), o la celebración, el mismo año, de la Eurocopa de fútbol en Portugal (Frois, 2008); ii) la proliferación de diferentes formas de identificación basadas en biométricos (Kokumai, 2016); iii) el desarrollo de identificadores más precisos para el control de personas en aduanas y puestos fronterizos (Salter, 2004; Valentín *et al*., 2016); iv) el incremento de los sistemas automáticos de escaneo (Kim *et al*., 2016); y, finalmente, v) la imprescindible extensión de la capacidad de los servidores para almacenar cantidades masivas de datos que se generan al día, del orden de 2,5 *exabytes*[8] en 2015, y consiguiente evolución de las metodologías que permiten trabajar con estas ingentes y crecientes cantidades de datos, que han tenido que superar las tradicionales técnicas de análisis de datos basadas en *data mining*, estadística o *machine learning*, entre otras (Bello-Orgaz *et al*., 2016).

La vigilancia masiva, denunciada por Snowden,[9] supera la concepción meramente espacial de lo público para instalarse

8 Un *exabyte* equivale a 10^{18} bytes

9 Véase «Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations», Glenn Greenwald, Ewen MacAskill y Laura Poitras, *The Guardian*, 11 de junio de 2013: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Véase también «Edward Snowden Comes Forward as Source of NSA Leaks», Barton Gellman, Aaron Blake y Greg Miller, *The Washington Post*, 9 de junio de 2013: <https://www.washingtonpost.

en un espacio-aparentemente-virtual, multiconectado de lo que se ha denominado IoT, un espacio con el que los sujetos interactúan, mediante uno o varios dispositivos, a veces de forma simultánea, durante las veinticuatro horas del día. Ello facilita un seguimiento completo del sujeto a través de los meandros de su vida cotidiana. El *panóptico benthamiano*, aquella metáfora del poder no-visible y omnisciente que recuperó Foucault en *Vigilar y castigar* (1975), da buena cuenta ahora del sistema de información conformado por los datos que voluntariamente suministramos sobre nuestros gustos, deseos, anhelos e ideas, pero también sobre los lugares que visitamos, el dinero del que disponemos o pedimos prestado, los libros que leemos, lo que compramos, etc.

> «De ahí el efecto más importante del Panóptico: inducir al detenido en un estado consciente e permanente de visibilidad que asegura el funcionamiento automático del poder […] Por ello, en tanto que el prisionero se sabe continuamente observado, la vigilancia puede considerarse, simultáneamente, deficiente y excesiva. Deficiente porque es esencial que se sepa vigilado sin saber él mismo quién le observa; excesiva, porque él ya no tiene necesidad de ser efectivamente vigilado. Por esto Bentham colocó el principio de que debía ser visible e inverificable. Visible: sin cesar, el detenido tendrá delante de los ojos la torre central desde donde es espiado. Inverificable: el detenido nunca debe saber si está siendo observado; solo deberá tener certeza de que siempre podrá serlo» (Foucault, 2002, págs. 166-167).

Si bien, más que la voluntad de aplicar la vigilancia en sí misma como un castigo, parece más adecuada la perspectiva que señala que aquella «voluntad de castigar» ha sido susti-

com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.6cbe73b654aa>

tuida por una «voluntad de controlar» (Deleuze, 1992, págs. 4-6). La famosa viñeta que Steiner publicó en *The New Yorker* en 1993, en la que un perro frente a un PC le dice a otro que le mira a su vez sentado en el suelo: «En internet, nadie sabe que tú eres un perro», no puede ser ya válida, aunque sí, desde luego, siga siendo pertinente el chiste.[10] Actualmente, BD nos permitiría conocer no solo que se trata de un perro, sino su raza, sus galletas favoritas, si ha ganado algún premio en algún concurso canino o, incluso, se aventurará a adivinar cuáles son las noticias que le harán reaccionar positivamente en Facebook, qué libros leerá o qué ropa comprará en los próximos meses.

¿Cómo afecta ese control a los derechos fundamentales? En primer lugar, por la falta de transparencia e información: el sujeto no sabe, habitualmente, que está siendo observado, monitorizado, quizá comentado, por lo que el sujeto no puede expresar ningún tipo de reacción o resistencia. El sujeto pasa a constituir un registro en cualquier base de datos de la que no tiene conocimiento, sin garantía de que de ese registro resulten consecuencias no previsibles. En lo imprevisible está el riesgo, no personalmente aceptado, no hay un consentimiento informado estricto, lo que afecta gravemente a su autonomía, como ciudadano, pero también como consumidor.

Las revelaciones de Edward Snowden demostraron que estas preocupaciones son reales y que las capacidades técnicas para recolectar, almacenar y buscar grandes cantidades

10 *Cfr.* «Nobody Knows You're a Dog: As Iconic Internet Cartoon Turns 20, Creator Peter Steiner Knows the Idea Is As Relevant As Ever», Michael Cavna, *The Washington post*, 31 de julio de 2013: <http://wpo.st/N8vJ2>

de datos sobre conversaciones telefónicas, búsquedas en internet y pagos electrónicos ya están en vigor y son usadas rutinariamente por los gobiernos. Para las empresas, los datos personales sobre clientes, fidelizados o potenciales, también son ahora un activo clave. Al mismo tiempo, el significado y el valor de la privacidad sigue siendo objeto de considerable controversia. La combinación del creciente poder de las nuevas tecnologías y la falta de transparencia sobre su funcionamiento y potencial están generando problemas relacionados con el derecho, la política y la ética.

De acuerdo con el estado de la cuestión realizado por Mortazavi y Salah (2015), es posible identificar los siguientes problemas entre privacidad y *big data* :

- Los usuarios no han llegado a comprender cómo afectan las violaciones de privacidad tanto a individuos como al comportamiento social de estos (Solove, 2011, págs. 32-34).
- Existe una falta de transparencia en cuanto a políticas de privacidad y de información respecto a los análisis predictivos aplicados a los datos facilitados por los usuarios, y esto debido a las carencias de los procedimientos legales relacionados con BD (Crawford; Schultz, 2014).
- Los datos falsos o los resultados de análisis falsos pueden ser compartidos (a menudo de forma automática) en los centros de datos, lo que dificulta que los usuarios puedan ejercer su derecho de corregir o enmendar los errores o falsedades que les afecten mediante un adecuado procedimiento. Otorgar al gobierno acceso no restringido a esta forma de vigilancia masiva abre la puerta a un estado de vigilancia, lo cual entraña un riesgo elevado para que la tiranía se implante de forma velada en

nuestros sistemas democráticos. De hecho, las agencias gubernamentales de investigación tienden a violar las expectativas razonables de privacidad si no hay barreras que impidan esta intromisión en la intimidad de las personas. BD hace que estos problemas cambien de escala, alcanzando unas dimensiones nunca vistas anteriormente (Citron; Gray, 2013).

- Es posible programar análisis de BD que permiten predecir con exactitud y de forma automática un amplio rango de atributos altamente sensibles como orientación sexual, etnicidad, creencias religiosas o ideología política, uso de sustancias adictivas, nivel de inteligencia, o rasgos personales del carácter como optimismo o tendencias depresivas, entre otros. Todos ellos pertenecen originalmente al ámbito de lo estrictamente íntimo y, por tanto, necesariamente privados (Kosinski *et al.*, 2013).
- Hay un desajuste de las políticas reclamadas por los proveedores, que aquí hemos denominado *comsumers*, y los controles reales disponibles para preservar la privacidad de los usuarios (Anthonysamy *et al.*, 2013; Martin, Murphy, 2017)
- Además, los proveedores disponen de un incentivo económico que favorece que estos cometan errores relacionados con la privacidad de sus usuarios, divulgando, compartiendo o cediendo los datos a terceros (Feldman *et al.*, 2012).
- Del mismo modo, existe un incentivo policial similar para utilizar técnicas avanzadas de vigilancia para recopilar datos de forma continua, incluyendo imágenes digitales. Además, la centralización de información incrementa el riesgo de ataques de intrusos a las colecciones de datos recopiladas y almacenadas por los gobiernos (Easton-Calabria, Allen, 2015; O'Leary, 2017).

- Existen limitaciones en algunas de las técnicas más avanzadas diseñadas para permitir el análisis de datos privados, limitaciones que hacen que estas técnicas sean vulnerables (Chaudhuri; Hsu, 2011).
- Actualmente existen leyes de privacidad de la información que se ven rápidamente superadas por el ritmo de cambio y de incremento de la complejidad de la tecnología, y que además ya no se ajustan al espíritu de las leyes originales, como por ejemplo la Cuarta Enmienda a la Constitución de los Estados Unidos,[11] en la prevención de violaciones del derecho y el interés de las personas a la privacidad (Warren; Brandeis, 1890).

En el capítulo 5, se analizan cómo se están confrontando estos problemas desde las instituciones públicas, tanto en Estados Unidos como en la Unión Europea; así como desde ámbitos profesionales, como la renovación participada del Código de ética y conducta profesional de la Association for Computing Machinery. Las conclusiones apuntarán hacia la responsabilidad que gobiernos, ciudadanía y comunidad científica deben asumir en la confrontación de estos problemas que afectan al corazón mismo de los sistemas democráticos.

11 La Cuarta Enmienda fue introducida en 1789, y aprobada definitivamente por el presidente Jefferson en 1792 como parte de la Carta de Derechos (*Bill of Rights*) redactados para controlar los abusos gubernamentales a los ciudadanos tras la Guerra de la Independencia: «El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas». Véase <https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv>

4. Propiedad de los datos: ¿derecho o interés?

En el caso de que una persona ceda intencionalmente cualquier información sobre su identidad privada, emerge una nueva cuestión ética: ¿qué derecho tienen otros a hacer dicha información pública? Aún más, si la transferencia de información privada a una base de datos responde a una intencionalidad que tiene por objeto atender nuestros intereses personales, ¿puede ser considerada la construcción de información de nosotros mismos un acto creativo? ¿Se transfieren en el mismo acto los datos y los derechos asociados a dicha creación? ¿Nuestra mera existencia constituye entonces un acto creativo? Si es así, entonces, ¿no deberían seguirse aquí todas las protecciones legales asociadas con la ley de derechos de autor?

¿Cuáles son las obligaciones y derechos de quienes generan los datos? ¿A quién pertenecen los datos? ¿A quiénes los generan o a quiénes pusieron el medio para hacerlos posibles? ¿Pueden los derechos de propiedad de los datos ser transferidos? ¿Y de quienes los utilizan y/o explotan? ¿Es necesario distinguir entre propiedad (*property*) y pertenencia (*ownership*)?

Un buen punto de partida para acometer estas cuestiones relacionadas con la propiedad de los datos generados durante nuestra interacción con los diferentes medios de información tecnológica podría ser la distinción entre *derecho* e *interés*, el planteamiento de la distinción fundamental respecto a la propiedad de los datos tiene que ver con la consideración de esta bien como un derecho o como un interés. Un derecho a la propiedad de los datos tendría una notación normativa asentada en la libre disposición de estos para hacer el uso de ellos que consideremos, ya sea de un modo personal, colecti-

vo o comunitario. Esta concepción de la propiedad exige una revisión de las regulaciones legales existentes.

Por otro lado, el interés vendría a significar un deseo de preservar la privacidad mediante la guarda y custodia de los datos que nos conciernen. Esta forma de considerar la propiedad está más relacionada con el concepto de privacidad abordado ampliamente en el epígrafe anterior y es el que consideramos aquí como reseñable respecto a las implicaciones éticas del uso de BD.

5. Hacia una gestión de la privacidad justa y equitativa: entre la ética y la ley

Una gestión justa y equitativa de los problemas antes citados, o de otros que no conforman ese listado urgente, exige una inteligente combinación entre ética, ley y decisiones políticas. Ninguna de ellas por sí sola será capaz de confrontar un problema tan complejo como el que abordamos, necesariamente de un modo superficial.

Guardar debido respeto y garantizar la preservación de la intimidad de las personas, aquello que actualmente denominamos privacidad, aparece ya con un valor moral inalienable en documentos del antiguo Egipto, China, Grecia y Persia. Los tratados tempranos sobre la privacidad aparecieron con el desarrollo de la protección de la privacidad en la ley estadounidense, justificándose en gran parte aludiendo a razones morales (Warren; Brandeis, 1890). En las discusiones en las que se ha abordado la privacidad en la época contemporánea, algunos la tratan como un interés con valor moral, mientras

que otros se refieren a ella como un derecho moral o legal que debe ser protegido por la sociedad y/o la ley.

Así, aunque sea complejo establecer una construcción unívoca del concepto, la mayoría considera que la privacidad es un concepto significativo y valioso para las personas. Desde el control de la información acerca de uno mismo, hasta ampliar el radio de acción afectado por el concepto, considerándolo algo ineludible para garantizar la dignidad de las personas. La relación, además, entre privacidad e intimidad garantiza el desarrollo de relaciones interpersonales variadas y significativas en tanto que es el puntal de muchas normas sociales que garantizan la convivencia cívica. Pero la privacidad también entraña un valor negativo para las personas, cuando se considera un pesado cortinaje tras el que ocultar la dominación, la degradación o el daño físico. Esto último ha sido especialmente argumentado por el pensamiento feminista y decolonialista, pero también por aquellos que denuncian los abusos que se dan en la red amparados por el anonimato de los agresores (Allen, 1988; 1990; 2011).

Una aplicación de los principios profesionales abordados en el capítulo anterior la encontramos en las siguientes razones morales para la protección de datos personales y para proporcionar control directo o indirecto sobre el acceso a esos datos por otros (Van Den Hoven, 2008).

- Prevención del daño: garantizar que las contraseñas de acceso a los sitios son seguras y que la geolocalización no es activada por los dispositivos sin el consentimiento del usuario, son dos formas inexcusables de evitar daños.
- Desigualdad informativa: los datos personales se han convertido en mercancías. Las personas suelen estar en posición

de desventaja para negociar contratos sobre el uso de sus datos y no tienen los medios para verificar si el proveedor cumple con los términos del contrato. Las leyes, la reglamentación y la gobernanza de la protección de datos tienen por objeto establecer condiciones equitativas para la redacción de contratos relativos a la transmisión y el intercambio de datos personales, así como la provisión de controles y garantías de reparación. Esto conlleva garantizar la redacción de contratos inteligibles para el usuario que velen por su seguridad y no solo por la del proveedor del servicio.

- Injusticia informativa y discriminación: la información personal proporcionada en un determinado contexto (por ejemplo, en atención médica) puede cambiar su significado cuando se utiliza en otro contexto (como las transacciones comerciales) y puede conducir a discriminación y desventajas para el usuario.
- Intrusión en la autonomía moral: la falta de privacidad puede exponer a los individuos a fuerzas externas que influyen en sus elecciones. Por ejemplo, Lazer y Bakshy *et al.* advirtieron en sus respectivos artículos publicados por la revista *Science*, en junio de 2015, de aquello que denominaron el advenimiento del *algoritmo social* y de las consecuencias que estaba teniendo su implantación en las redes sociales más populares como Facebook y Twitter (Bakshy *et al.*, 2015; Lazer, 2015). El sesgo ideológico al que aludían estos autores ha devenido realidad durante la campaña presidencial en los Estados Unidos de 2016. Las noticias falsas, apoyando al candidato republicano o bien calumniando a la candidata demócrata, han conseguido ser las más difundidas gracias a lo que se denomina la *burbuja del filtro*. Los algoritmos sociales, obviando la autonomía de los usuarios, solo

muestran aquellas *entradas* con las que los usuarios podrían estar potencialmente de acuerdo, porque son las más populares entre los miembros de su comunidad, desechando aquellas que podrían generar conflicto. Muchos analistas han denunciado que este modo de gestionar las noticias, permitiendo que tanto aquellas «verdaderas» como otras manifiestamente «falsas» sean consideradas por el algoritmo en igualdad de condiciones, ha servido para que Donald Trump llegue a ser presidente. Un fenómeno que ha llevado a establecer el potencial de lo que ya se conoce como *posverdad*, que ampara lo que podríamos llamar la certeza de las mentiras, y que ha ganado la posición de palabra del año 2016 otorgada por el *Oxford Dictionary*.[12]

Una gestión irresponsable de la privacidad provoca que los riesgos de daño, desigualdad, discriminación y pérdida de autonomía emerjan fácilmente. Algo que afecta necesariamente no solo a la integridad de las personas, sino que degrada sistemáticamente la cohesión social. Se ha argumentado que el principio de precaución, bien conocido en la ética ambiental, podría tener un papel determinante también en la ética aplicada a las tecnologías de la información. El principio velaría por establecer relaciones de poder equitativas entre *pro* y *comsumers*, que evitarían que la sobrecarga moral recaiga principalmente en unos o en otros. Aparte de los debates generales sobre las características deseables e indeseables del principio de precaución, los retos que se plantean son su

12 Véase «The failure of Facebook democracy», N. Heller, *The New Yorker*, 18 de noviembre de 2016: <http://www.newyorker.com/culture/cultural-comment/the-failure-of-facebook-democracy>

traducción a los efectos sociales, así como su aplicación a las consecuencias inducidas por las acciones intencionales de los agentes (Pieters; Van Cleeff, 2009).

Por otro lado, casi todos los países disponen de leyes de protección de datos en vigor.[13] El principio moral básico subyacente a estas leyes es el requisito del consentimiento informado suscrito por el interesado para autorizar el almacenamiento y tratamiento de los datos. Además, el procesamiento de información personal requiere que se especifique su propósito, se limite su uso, se notifique a los individuos y se les permita corregir inexactitudes. El proveedor del servicio, ya sea una red social, un organismo oficial de ciudanía digital o un gestor de dispositivos como Apple o Android, lo que hemos denominado aquí *comsumer*, será el responsable último ante las autoridades.[14] Debido a que es imposible garantizar el cumplimiento de todos los tipos de procesamiento de datos en todas estas áreas y aplicaciones con estas normas y leyes de manera tradicional, se espera que las llamadas tecnologías de mejora de la privacidad y sistemas de gestión de identidad reemplacen a la supervisión humana en muchos casos. El desafío con respecto a la privacidad en el siglo XXI es asegurar que la tecnología esté diseñada de tal manera que incorpore requisitos de privacidad en el *software*, la arquitectura, la infraestructura y los procesos de trabajo de tal manera que sea mínimamente

13 Véase el informe sobre el estado de la cuestión de la Agencia Española para la Protección de Datos: <http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php>

14 Véase *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Co-operation and Development (OECD): <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>

probable que ocurran violaciones a la privacidad, al menos de forma sistemática.[15]

Solove (2011) ha propuesto una taxonomía de la vulnerabilidad de la privacidad, de acuerdo con los diferentes momentos que afectan a los procesos de información: i) *recolección* se refiere a la vigilancia e interrogación con objeto de captar datos; ii) *proceso* se refiere a la recopilación, identificación, inseguridad, uso secundario y exclusión; iii) *difusión* afecta a violaciones de confidencialidad, revelación y exposición indebida, facilidad de acceso, chantaje, apropiación y distorsión; y, finalmente, iv) *intrusión e interferencia en la toma de decisiones* son las dos principales formas de vulneración de la privacidad. El segundo de ellos es quizá el más difícil de comprender, aunque aquí ya hemos visto varios ejemplos relacionados con el rol que asumen los algoritmos en las redes sociales o en los buscadores y la limitación en el ejercicio de la autonomía personal que ello implica.

Por último, es importante considerar los dos enfoques que se plantean en Europa y Estados Unidos respecto a la privacidad y las tecnologías de la información. Así, mientras en Europa se conceptualiza la privacidad en términos de *protección de datos*, en Estados Unidos se aborda en términos de *privacidad*, sin abordar propiamente cuál es el objeto de protección y qué medios técnicos pueden contribuir a proteger los datos. Por su parte, la noción de protección de datos es de gran ayuda, ya que no solo da una imagen relativamente clara del

15 Existen organizaciones no gubernamentales cuyo objetivo es, precisamente, desarrollar soluciones tecnológicas a los problemas de privacidad generados por esa misma tecnología. Véase, por ejemplo, el Electronic Privacy Information Center, con sede en Washington y que cuenta en su consejo asesor con profesores universitarios, investigadores, periodistas o fundadores de otras tantas organizaciones no gubernamentales como Data & Society o Black Girls Code: <https://epic.org>

problema, sino que invita a proponer diferentes respuestas a la cuestión que plantea por qué los datos deben ser protegidos.[16]

El reto que supone una gestión equitativa y justa de la privacidad comienza, precisamente, por conocer el alcance del problema y disponer de suficientes medios y audacia para adelantarse a los nuevos problemas que surgirán a medida que la tecnología mantenga su línea de transformación y creciente complejización. Es evidente que la privacidad es quizá el problema más acuciante en lo que respecta a BD y derechos civiles (Easton-Calabria; Allen, 2015). Esto debería ser razón suficiente para que los gobiernos garanticen el desarrollo y aprobación de nuevos sistemas de leyes, o bien se diseñen nuevas tecnologías que ayuden a prevenir la destrucción de nuestras valiosas reglas de civilización, al mismo tiempo que se garantiza que la evolución de *big data* enriquece nuestras vidas tanto social como individualmente.[17]

16 *Cfr*. El marco jurídico fundamental para la regulación de los servicios *online* en la Unión Europea, incluyendo el comercio electrónico, es la Directiva 2000/31/EC: <http://ec.europa.eu/internal_market/e-commerce/index_en.htm>. La Estrategia Europea para una Comunicación Segura (2006): <http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766>. De estos dos modos de comprender la privacidad da cuenta la editorial de *The Washington Post* del día 9 de octubre de 2015, «European Ruling is Merely a Symbolic Victory for Privacy», y la respuesta de varios expertos estadounidenses a esta editorial, publicada en ese mismo medio el día 13 de octubre de 2015, «Digital Privacy, in the U.S. and Europe»: <http://www.nytimes.com/2015/10/09/opinion/european-ruling-is-merely-a-symbolic-victory-for-privacy.html?_r=0> y <http://www.nytimes.com/2015/10/13/opinion/digital-privacy-in-the-us-and-europe.html?_r=0>, respectivamente

17 A este respecto son reseñables los informes periódicos que, desde 2014, ha hecho públicos el Big Data Working Group de la administración del presidente Barack Obama: «Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights», Executive Office of the President, mayo de 2016: <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>

Todos los problemas mencionados, y que en muchas ocasiones afectan del mismo modo a unos y a otros, deben abordarse desde la premisa planteada por la distinción radical que se establece entre el mundo real, *offline*, y en mundo virtual, *online*. Ni las expectativas, ni las exigencias de derechos, ni los intereses, se ven suficientemente identificados entre las dos formas actuales de estar-en-el-mundo, lo que plantea no pocas dificultades a la hora de gestionar los problemas, esencialmente el de la privacidad y la intimidad de las personas, de un modo equitativo y justo. La ética en este aspecto puede, y debe, superar a la ley en el logro de objetivos, en tanto que el poder legislativo, al menos tal y como ha sido concebido hasta el momento, no puede adaptarse ni al volumen ni a la velocidad de cambio de escenarios y contextos en los que se mueve *big data*.

Bibliografía

Allen, A. L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa: Rowman & Littlefield.

Allen, A. L. (1990). «Coercing Privacy». En: *William and Mary Law Review* (n.º 40, págs. 723-757).

Allen, A. L. (2011). *Unpopular Privacy: What Must We Hide?* Oxford: Oxford University Press.

Anthonysamy, P.; Greenwood, P.; Rashid, A. (2013). Social Networking Privacy: Understanding the Disconnect from Policy to Controls. En: *IEEE Computer* (vol. 46, n.º 6, págs. 60-67).

Bakshy, E.; Messing, S.; Adamic, L. A. (2015). «Exposure to Ideologically Diverse News and Opinion on Facebook». En: *Science* (vol. 348, *issue* 6.239, págs. 1.130-1.132).

Bauman, Z. (2003). *Comunidad, en busca de seguridad en un mundo hostil*. Madrid: Siglo XXI Editores.

Bell, G.; Gemmell, J. (2010). *Your Life, Uploaded: The Digital Way to Better Memory, Health, and Productivity*. Nueva York: Penguin Books.

Bello-Orgaz, G.; Jung, J. J.; Camacho, D. (2016). «Social Big Data: Recent Achievements and New Challenges». En: *Information Fusion* (n.º 28, págs. 45-59).

Chaudhuri, K.; Hsu, D. (2011). «Sample Complexity Bounds for Differentially Private Learning». En: *Colt* (vol. 19, págs. 155-186).

Citron, D.; Gray, D. (2013). «The Right to Quantitative Privacy». En: *Minnesota Law Review* (vol. 98, págs. 62-144).

Crawford, K.; Schultz, J. (2014). «Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms». En: *Boston College Law Review* (vol. 55, n.º 1, págs. 93-128).

Davis, K.; Patterson, D. (2012). *Ethics of Big Data*. Sebastopol: O'Reilly Media Inc.

Deleuze, G. (1992). «Postscript on the Societies of Control». En: *October* (vol. 59, págs. 3-7).

Easton-Calabria, E.; Allen, W. L. (2015). «Developing Ethical Approaches to Data and Civil Society: From Availability to Accessibility». En: *Innovation-the European Journal of Social Science Research* (vol. 28, n.º 1, págs. 52-62).

Foucault, M. (1975). *Vigilar y castigar*. Buenos Aires: Siglo XXI Editores, 2002.

Frois, C. (2008). «Bases de dados, pessoas e sistemas de vigilância em Portugal: análise de um processo em transição». En: C. Frois (ed.). *A sociedade vigilante. Ensaios sobre Identificação, Vigilância e Privacidade* (págs. 111-132). Lisboa: Imprensa de Ciências Sociais.

Frois, C. (2011). *Vigilância e poder*. Lisboa: Mundos Sociais.

Kapferer, B. (2004). «The New Leviathan and the Crisis of Criticism in the Social Sciences». En: B. Kapferer (ed.). *The World Trade Center and Global Crisis. Some Critical Perspectives* (págs. 79-85). Nueva York: Berghahn Books.

Kim, J.; Udpa, L.; Kim, J. (2016). «Development and Application of Arduino Based Scanning System for Non-destructive Testing». En: *International Journal of Applied Engineering Research* (vol. 11, n.º 14, págs. 8.217-8.220).

Kokumai, H. (2016). «Biometrics: Great for Physical Security, Possibly a Big Mistake for Cyber Security?». En: *Biometric Technology Today* (n.º 5, págs. 7-9).

Kosinski, M.; Stillwell, D.; Graepel, T. (2013). «Private Traits and Attributes are Predictable from Digital Records of Human Behavior». En: *Proceedings of the National Academy of Sciences* (vol. 110, n.º 15, págs. 5.802-5.805).

Lazer, D. (2015). «The Rise of the Social Algorithm». En: *Science* (vol. 348, n.º 6.239, págs. 1.090-1.091).

Lyon, D. (1994). *The Electronic Eye. The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Martin, K. D.; Murphy, P. E. (2017). «The Role of Data Privacy in Marketing». En: *Journal of the Academy of Marketing Science* (vol. 45, n.º 2, págs. 135-155).

Marx, G. T. (1988). *Undercover. Police Surveillance in America*. Berkeley: University of California Press.

Mason, R. O. (1986). «Four Ethical Issues of the Information Age». En: *Management Information Systems Quarterly* (vol. 10, n.º 1, págs. 5-12).

McCahill, M. (1998). «Beyond Foucault: Towards a Contemporary Theory of Surveillance». En: C. Morris; J. Moran; G. Amstrong (eds.). *Surveillance, Close Circuit Television and Social Control* (págs. 41-65). Aldershot: Ashgate Publishing Group.

Morozov, E. (2015). «La condición superhumana». En: *La locura del solucionismo tecnológico* (págs. 209-349). Madrid: Katz Editores.

Mortazavi, M.; Salah, K. (2015). «Privacy and Big Data». En: S. Zeadally; M. Badra (eds.). *Privacy in a Digital, Networked World* (págs. 38-55). Berlín: Springer.

Norris, C.; Armstrong, G. (1999). *The Maximum Surveillance Society. The Rise of Close Circuit TV in Britain*. Londres: Berg.

O'Leary, R. (2017). «The New Guerrilla Government: Are Big Data, Hyper Social Media and Contracting Out Changing the Ethics of Dissent?». En: *PS-Political Science & Politics* (vol. 50, n.º 1, n.º 12-22).

Pieters, W.; van Cleeff, A. (2009). «The Precautionary Principle in a World of Digital Dependencies». En: *Computer* (vol. 42, n.º 6).

Rule, J. (1973). *Private Lives and Public Surveillance*. Londres: Allen Lane.

Salter, M. B. (2004). «Passports, Mobility and Security: How Smart Can the Border Be?». En: *International Studies Perspectives* (vol. 5, n.º 1, págs. 71-91).

Samatas, M. (2004). *Surveillance in Greece. From Anticommunist to Consumer Surveillance*. Nueva York: Pella.

Solove, S. J. (2011). *Nothing to Hide*. New Haven: Yale University Press.

Taylor, L. (2016). «The Ethics of Big Data as a Public Good: Which Public? Whose Good?». En: *Philosophical Transactions of the Royal Society a-Mathematical Physical and Engineering Sciences* (vol. 374, n.º 2.083).

Trías, E. (2000). *Ética y condición humana*. Barcelona: Ediciones Península.

Valentín, K.; Wild, P.; Štolc, S.; Daubner, F.; Clabian, M. (2016). «Optical Benchmarking of Security Document Readers for Automated Border Control». En: *SPIE Security+ Defence* (999502-999502-11).

Van Den Hoven, J. (2008). «Information Technology, Privacy and the Protection of Personal Data». En: J. Van Den Hoven; J. Weckert (eds.). *Information Technology and Moral Philosophy* (págs. 301-322). Cambridge: Cambridge University Press.

Warren, S. D.; Brandeis, L. D. (1890). «The Right to Privacy». En: *Harvard Law Review* (págs. 193-220).

Westin, A. (1967). *Privacy and Freedom*. Nueva York: Atheneum.

Capítulo IV

La toma de decisiones éticas en el entorno de la IoT y *big data*

1. Introducción

La recolección, registro, análisis y utilización de los datos afectan e implican significativamente a las personas y a las relaciones que establecen entre ellas. Las personas y las comunidades en las que se organizan adoptan valores y principios morales que establecen un acuerdo, no escrito, de mínimos, que garantiza la convivencia pacífica. Los principios de esa ética cívica deben ser acordados mediante la deliberación pública. El uso público de la razón como herramienta para el logro de consensos en áreas tan dispares como la biotecnología, la nanotecnología, la gestión ambiental, el cambio climático, la educación o las actividades empresariales, ha sido teorizado y desarrollado en las denominadas éticas aplicadas a estas actividades humanas, especialmente a partir del último tercio del siglo XX (Cortina, 2002).

Para lograr esa deliberación pública que permita tomar decisiones que influyan en el desarrollo de esos campos se precisa, en primer lugar, una sociedad civil como parte de una «sociedad bien ordenada», en términos rawlsianos:

> «En una sociedad bien ordenada los ciudadanos sostienen los mismos principios de derecho y tratan de alcanzar el mismo juicio en los casos particulares […] Por otra parte, las personas encuentran su bien de distintos modos, y para

> una persona pueden ser buenas muchas cosas que no lo serían para otra. Además, no es urgente alcanzar un juicio públicamente aceptado acerca de lo que es el bien de unos individuos en particular. Las razones que hacen necesario tal acuerdo en cuestiones de justicia no constituyen juicios de valor» (Rawls, 1971, págs. 405-406).

No olvidemos que, de acuerdo con esta teoría, en esta sociedad las instituciones «son justas, y este hecho es públicamente reconocido. Sus miembros tienen también un claro sentido de la justicia, un deseo efectivo de obedecer las reglas existentes, y de dar a cada uno lo que tienen derecho. En este caso, podemos suponer que todos tienen el mismo valor moral» (Rawls, 1971, pág. 289). La concepción de la justicia de Rawls podría resumirse en dos puntos: primero, que las normas que permiten la justicia deben ser hechas por y para las personas, y no al contrario; y segundo, que la justicia exige publicidad, esto es, transparencia, y reciprocidad. Así, reconociendo que los proyectos de vida de los individuos son diferentes, se admite la capacidad de dichos individuos para llegar a establecer juicios comunes sobre casos particulares por los que se ven afectados.

Una de las teorías que ha trabajado por incorporar estas concepciones abstractas de la justicia al ejercicio práctico de la ética, en particular de la ética empresarial, es la teoría de los grupos de interés o *stakeholders*.

La definición más extendida del término fue formulada por Freeman (1994), quien considera *stakeholder*[1] como «cualquier

1 El término, empleado por primera vez en el memorando sobre empresa publicado por el Standford Research Institute en 1963, procede de un juego de palabras con el que se pretendía dar respuesta a la tendencia principal en la dirección de empresas en los años sesenta, en la que se consideraba que los *stockholders* —accionistas— eran los únicos con intereses legítimos sobre la actividad de las empresas.

grupo o individuo que pueda afectar o ser afectado por el logro de los objetivos empresa» (Freeman, 1994, pág. 24). En cuanto que el logro de los objetivos de cualquier organización son fundamentales las decisiones y las políticas adoptadas, se trata de una definición que contiene un sentido de reciprocidad entre actores y con ello de necesaria e ineludible relación y comunicación. Una empresa u organización que adopte este enfoque va más allá de la vigilancia estricta de la cuenta de resultados (Tuleja, 1987), adoptando planteamientos ético-normativos que «permiten comprender que entre los diferentes *stakeholders* que configuran la empresa se establecen una serie de relaciones que pueden ser entendidas desde la perspectiva no solo del contrato jurídico o del contrato social, sino del contrato moral» (González, 2007, pág. 209).

No debe extrañar entonces que las primeras disciplinas que han incorporado esta teoría para abordar la compleja interacción de actores sociales afectadas por su actividad en el entorno de la IoT y de los BD hayan sido el neuromárketing (Aghazadeh, 2017; Pop *et al.*, 2017), los estudios sobre la toma de decisiones en el consumo y la producción sostenibles (Tseng; Chiu; Liang, 2017), o los análisis de redes sociales (Aghazadeh, 2017; García-Crespo *et al.*, 2017). La extensión en la aplicación de esta teoría a ámbitos no empresariales ha sido recomendada especialmente a entidades no lucrativas e instituciones públicas (Phillips *et al.*, 2003; Saz, 2008); de

La adopción del término *stakeholder*, literalmente 'depositario de una apuesta', tenía como objeto el reconocimiento de que en las organizaciones existen una gran variedad de intereses en juego que atienden a un complejo sistema de relaciones y que estos intereses podían proceder de otros tantos actores que intervenían de algún modo en la actividad desarrollada por dicha organización (Etzioni, 1998, pág. 682).

forma más específica, se ha sugerido su implementación en todas aquellas en las que sea imprescindible la adopción de una visión estratégica de gestión a largo plazo (McAdam; Scott, 2005).

2. Aplicación de la teoría de los *stakeholders* a la toma de decisiones en el entorno de la IoT y *big data*

Dar una respuesta eficaz ante la posible pluralidad de demandas es necesario que desde la dirección de las organizaciones se identifique correctamente a cada uno de los *stakeholders* realizando un análisis individualizado de sus cualidades para, de este modo, conocer con mayor precisión las expectativas que pueden tener con respecto a la estrategia de la organización (Caballero *et al.*, 2008), una estrategia que debería ser diseñada atendiendo a las relaciones que se establecen con y entre los *stakeholders*, así como a su diversidad y complejidad (Wisniewski; Stewart, 2004). Esta concepción cobra mayor sentido en el ámbito del sector público, ya que se tiene aquí la responsabilidad de responder y dar servicio al conjunto de los ciudadanos, y por tanto de demostrar que los objetivos están siendo conseguidos. Nada más propio del enfoque que atender la satisfacción de los intereses de los *stakeholders* que le dan legitimidad y que le proporcionan los recursos (Shenkar; Yuchtman, 1997).

Proponemos, por tanto, en este caso, la aplicación de la teoría de los *stakeholders* para realizar una gestión eficiente y ética de los escenarios que se generan en el curso de la reco-

pilación, registro, análisis y uso de datos. Un enfoque gerencial que supone la necesidad de identificar los distintos grupos de interés afectados, para atender de forma simultánea sus intereses legítimos con el ánimo de buscar el equilibrio entre los objetivos del sector público y/o privado, y de las distintas partes interesadas, esencialmente de la ciudadanía. Ello supondrá identificar sus implicaciones en la estructura organizativa, en la definición de las políticas a seguir y su consideración en la toma de decisiones. La teoría de los *stakeholders* se sustenta sobre la base de su exactitud descriptiva, su poder instrumental y validez normativa (Donaldson *et al.*, 1995, págs. 66-69).

La identificación de los *stakeholders* es una tarea compleja por la diversidad de intereses que se ponen de manifiesto, pero aún es mayor en el ámbito de la gestión de los sistemas de información por la multiplicidad de identidades y roles, la fragmentación de la responsabilidad y la indefinición de las consecuencias finales de las acciones ejecutadas por los diferentes grupos de interés. Una vez comprendida la pertinencia de la aplicación del enfoque de los *stakeholders*, asumimos las preguntas clave planteadas por Freeman para hacer efectiva esta aplicación:

> «¿Quiénes son aquellos grupos o individuos que pueden afectar o ser afectados por el logro de los objetivos de la organización? ¿Cómo podemos construir un mapa de *stakeholders* de la organización? ¿Cuáles son los problemas de construcción de este mapa?» (Freeman, 1984, pág. 54).

Para el descubrimiento y análisis de los grupos de interés se ha adoptado la aplicación de una propuesta de identificación dinámica en el tiempo (Wartick; Wood, 2000, págs.

93-115) que asigna los siguientes atributos o categorías a los *stakeholders*:

- El *stakeholder* se define como una persona, o grupo, capaz de afectar o ser afectado por la organización, es decir, es un sujeto que es interpelado por la actividad de dicha organización y que es, a su vez, «influyente», bien porque tiene poder efectivo, bien porque tiene habilidades o recursos que puede hacer valer ante la organización y afectar así a su funcionamiento. Un poder en el que es posible distinguir, a su vez, las tipologías de «poder coercitivo, poder utilitario y poder normativo-social» (Wood; Jones, 1995, pág. 260).
- La urgencia con la que los *stakeholders* pueden elevar o, de hecho, elevan ante el gestor sus intereses. La urgencia puede determinarse por la capacidad de presión, determinada por su intensidad y el tiempo durante el que se hace efectiva (Mitchell *et al.*, 1997, pág. 867).
- Finalmente, los *stakeholders* quedan definidos no únicamente por su poder y su urgencia, sino también por «el grado de legitimidad de sus demandas y por el grado y tipo de responsabilidad que la empresa tiene frente a tales intereses» (Mitchell *et al.*, 1997, pág. 858). Efectivamente, para recoger el planteamiento moral de la teoría era preciso no atender a cualquier tipo de interés, sino a aquellos intereses que sean legítimos por sí mismos o que el *stakeholder* esté legitimado para reclamar y defender. La legitimidad puede ser, a su vez, legal o moral.

Una vez valorados los *stakeholders* en función de estos tres atributos, es posible clasificarlos de acuerdo al número de atributos o categorías que los definan (Agle *et al.*, 2000):

- Los *stakeholders latentes* son aquellos que solo han sido valorados en una de las tres categorías. En el momento en el que se ha realizado el análisis no tienen relevancia para la actividad de la empresa, pero eso no quiere decir que no la puedan tener en un futuro mediante la adquisición de otros atributos.
- Los *stakeholders expectantes* son aquellos que han sido valorados en dos de los tres atributos, su relevancia para la empresa es considerada como moderada, si bien es habitual que se presenten ante la empresa como definitivos, por su afinidad con los intereses de esta, o bien generen alianzas con otros que estén en su misma situación para llegar a adquirir el atributo que les falta para alcanzar el siguiente nivel de influencia.
- Finalmente, los *stakeholders definitivos* son aquellos que logran ser valorados en las tres categorías, alcanzando por tanto el máximo nivel de influencia en la empresa.

Consideramos que la aplicación de estas estrategias para la identificación y clasificación de los grupos de interés que afectan a la gestión en aquellos escenarios que se generan bien durante la recopilación, registro, análisis y/o uso de datos, puede contribuir a facilitar la toma de decisiones participadas, incrementando así la transparencia y la gobernanza, y con ello la confianza y la conformación de un escenario cívico-*éthos* en el entorno de la IoT y BD.

3. La toma de decisiones éticas y sus implicaciones

Es importante no perder de vista que en este escenario la visión, la comprensión e, incluso, las intuiciones humanas siguen siendo imprescindibles. Para las decisiones particularmente importantes, la organización precisará de empleados que sepan hacerse preguntas sobre el problema en cuestión, y especialmente, tener habilidad para saber qué preguntas se les pueden plantear a los datos con el objeto de conseguir respuestas eficaces para la organización (McAfee *et al.*, 2012).

Tomar decisiones éticas dentro de una organización pondrá a funcionar nuestras habilidades y capacidades para alinear aquello que hemos identificado como valioso, con la cultura y los intereses de la organización para la que trabajamos, y las acciones que hagan real lo anterior. Es una labor que exige atención, reflexión y decisión por parte de los profesionales implicados, pero también un compromiso por parte de las organizaciones (Davis; Patterson, 2012). De hecho, la cultura de una organización permite hacer explícitos aquellos valores que los miembros de dicha organización sostienen en común (Bass, Avolio, 1993; Beckhard, 1969). Dichos valores y el desarrollo de una visión común de las acciones que la organización toma para hacer realidad esos valores mediante su actividad, influirá ineludiblemente en cómo concibe y trata la identidad, la privacidad y la gestión de la propiedad de los datos de sus usuarios, y en cómo entiende los impactos potenciales en la reputación del cliente (Certo, 2003). También es la vía más segura para garantizar el compromiso de sus empleados (Ramdhani *et al.*, 2017), especialmente para

asegurarse que se generan espacios para el aprendizaje conjunto y el intercambio de conocimientos (Pool, 2000).

Por ello, aquellas organizaciones que asuman con fluidez esta ineludible ética de los BD, adquirirán el valor estratégico de asumir un papel de líderes en la conducción de la alineación de valores y acciones éticas. Los procedimientos que podrían facilitar esta alineación son la transparencia, el conocimiento, preciso y actualizado, de la legislación y de los códigos éticos que afectan a los profesionales que intervienen en estos escenarios, así como una estimación honesta de las implicaciones a largo plazo que el uso de las tecnologías relacionadas con la IoT y los BD puedan llegar a transformarse en riesgos para la integridad, la dignidad o el derecho a la intimidad o la privacidad de las personas.

Diseñar innovaciones técnicas, desarrollar nuevas características de producto o tomar decisiones sobre la gestión tienen implicaciones éticas, independientemente de que se las considere o no. Ignorándolas no se las hace desaparecer, más bien al contrario, se incrementan las consecuencias negativas que estas puedan tener en la sociedad. Desafortunadamente, esta falta de consideración de los aspectos éticos de la toma de decisiones acerca de las prácticas de manejo de los datos es muy común. Una encuesta realizada por Lewis PR, en 2015, sobre el rendimiento de compañías B2B, B2C[2] y opera-

2 Esta clasificación atiende a los siguientes criterios: i) B2B o *business to business*, que no se encuentra limitada al entorno electrónico, sino que hace una referencia al origen y destino de una actividad que se aplica a la relación entre un fabricante y el distribuidor de un producto y también a la relación entre el distribuidor y el comercio minorista; ii) B2C o *business-to-consumer*, se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o usuario final. En la práctica, suele referirse a las plataformas virtuales utilizadas en el

doras en diferentes áreas, solo otorga a Microsoft y Samsung un mero aprobado (5) en transparencia.[3] Esto implica que aunque la mayoría de las empresas entienden que la gente se preocupa por su privacidad, no tiene una declaración clara de aquellos valores que sus políticas de privacidad apoyan o por qué los apoyan. Este ejemplo está tomado de Davis y Patterson (2012).

Big data facilita información mucho más precisa y exacta sobre los intereses y los gustos de los usuarios e incluso tienen un carácter predictivo, aunque este pueda incurrir en determinismo, como ya se ha señalado aquí antes. Ahora BD facilita información correlacionada entre compras realizadas y soñadas, gracias a las *wishlists* pero también por los enlaces de publicidad que nos animamos a abrir cuando navegamos por la red, cómo reaccionamos en Facebook ante las publicaciones de nuestras amistades o qué contenidos nos animamos a compartir en Twitter, entre otras muchas acciones interconectadas. Todo ello facilita una información privilegiada no solo sobre comportamientos y acciones sino sobre cómo influir mejor en sus decisiones futuras, ello implica una

comercio electrónico para comunicar empresas (vendedoras) con particulares (compradores). Por eso, el uso más frecuente es comercio electrónico B2C; y iii) B2B2C o *business to business + business to consumer*: este modelo designa una modalidad de comercio electrónico que agrupa el B2B y el B2C. Se trata de una versión más sofisticada de lo que podría ser la simple superposición de los dos negocios. Con la misma plataforma *online* y la misma plataforma de distribución, se trata de cerrar la cadena de valor completa, desde que un producto o servicio se fabrica hasta que llega al consumidor final.

3 Véase la interpretación completa de los resultados de la encuesta en «Poniendo nota a las tecnológicas en transparencia e innovación», Mónica Tilves, 28 de octubre de 2015: <http://www.silicon.es/poniendo-nota-a-las-tecnologicas-en-innovacion-transparencia-y-algo-mas-infografia-90143>

extraordinaria evolución de las estrategias de negocio, que son ahora más precisas y exactas y, por tanto, más efectivas.

En 1987, el presidente Ronald Reagan propuso a Robert Bork como miembro de la Corte Suprema. Su candidatura fue muy discutida tanto entre los demócratas como entre algunos republicanos. Su capacidad fue cuestionada, entre otras cosas, porque el *Washington City Paper* hizo público su historial de alquiler de vídeos. Bork no consiguió finalmente acceder a la Corte Suprema pero el caso impulsó la aprobación en 1988 de la *Video Privacy Protection Act* (VPPA) que hizo ilegal revelar información de historial de alquiler a terceros (Richards, 2014, pág. 62).

En septiembre de 2011, Netflix publicó un llamamiento público a sus clientes con intención de conseguir una enmienda a la VPPA que permitiese a sus usuarios compartir su historial de visualización en Facebook.[4] Solo veintitrés años después de la aprobación de la VPPA, cuyo objetivo era la protección de los consumidores y evitar que su historial de compra pudiese ser utilizado para juzgar sus capacidades profesionales, una empresa estadounidense estaba pidiendo apoyo a sus clientes, a los que la VPPA pretendía proteger, para permitir que la información sobre su historial de visualización de contenidos en *Netflix* fuese compartida legalmente. Este caso muestra hasta qué punto, y en poco más de veinte años, el escenario de la IoT ha influido en la conformación de nuestros valores y aquello que creemos que es realmente importante para nuestra propia vida. Son precisamente estos casos los que nos permiten comprender la paradójica

4 Citado por Davis y Patterson (2012, pág. 22). No nos ha sido posible acceder a la entrada de blog que Davis citaba como fuente: <http://blog.netflix.com/2011/09/Help-us-bring-facebook-sharing-to.html>

conexión que existe en demasiadas ocasiones entre los valores que operan en la vida cotidiana y el escenario que deriva de la IoT y de los BD. Este motivo ya justifica la necesidad de una discusión más explícita sobre el uso ético de la tecnología asociada a BD y del necesario equilibrio entre los beneficios de la innovación y el riesgo de daño.

4. Puntos de decisión ética: un marco para la toma de decisiones

Los puntos de decisión ética proporcionan un marco para explorar la relación entre los valores que entendemos sostienen nuestra vida como individuos en sociedad —y como miembros de una empresa u organización— y las acciones que resultan de las tomas de decisión, esto es, la construcción y administración de productos y servicios que utilizan tecnologías de BD. Los puntos de decisión ética se articulan en cuatro actividades que deben entenderse conectadas en bucle, esto es, de un modo no-lineal: i) investigación, ii) análisis, iii) articulación, y iv) acción.

La investigación trata sobre la indagación, discusión y establecimiento de los valores que la organización establece como parte de su cultura y, con ello, de su identidad. Ello implica una comprensión honesta de lo que las organizaciones realmente consideran son sus valores, y no tanto lo que creemos que son, o lo que entendemos que nuestros usuarios o clientes piensan que son. Para ello es necesario conformar equipos que sean capaces de trazar estrategias claras y sencillas que expliquen, analicen, dónde se alinean los valores y las

acciones —y también dónde no lo hacen—, o sobre cómo mantener o mejorar esa alineación a medida que las condiciones cambian con el tiempo.

Los puntos de decisión ética generan un nuevo tipo de capacidad organizativa: la capacidad de conducir una investigación ética y facilitar el diálogo ético. Tal investigación y discusión es difícil, no solo porque viene cargada con los sistemas de valores personales de las personas que conforman los equipos, sino también porque históricamente los negocios no se han enfocado en desarrollar capacidades organizacionales para facilitar tales actividades. *Big data* está llevando los valores y la ética a los procesos de diseño de productos y servicios, especialmente porque las consecuencias de las acciones que promueven tienen una escala de impacto mucho mayor de lo que las empresas imaginaron antes, lo que afecta a una amplia variedad de capacidades operacionales que históricamente los negocios no han desarrollado de un modo suficientemente honesto y comprometido. *Big data* está expandiendo la esfera de donde necesitamos aplicar el pensamiento de valor y con ello la ética aplicada. No porque la tecnología que emplea *big data* sea intrínsecamente peligrosa, o porque esté mal entendida, sino porque el volumen, la variedad y la velocidad de los datos que recopila, analiza y proporciona ha penetrado en la vida cotidiana de las personas de un modo nunca visto hasta ahora.

Big data afecta a los aspectos sociales, políticos, financieros y de comportamiento de nuestras vidas con nuevas consideraciones para la misma manera en que entendemos y estamos de acuerdo sobre el significado de palabras importantes como la identidad, la privacidad, la propiedad y la reputación. El reto no es entender cómo modificar esas palabras para

incorporar los cambios que aporta *big data*, pero tampoco pretender adaptar los cambios generados a nuestra comprensión histórica de esas palabras. El reto es desarrollar unas capacidades que permitan incorporar la investigación ética en nuestro curso normal de hacer negocios. Una investigación que es una forma de hablar de nuestros valores en el contexto de las acciones que tomamos en relación con las oportunidades que proporciona *big data*.

Aprender a reconocer y a comprometerse activamente con los puntos de decisión ética es una manera de empezar a construir esas capacidades. El marco básico nos ayuda a identificar cuáles son nuestros valores en realidad, a entender si se alinean con la forma en que estamos utilizando (o la intención de utilizar) *big data*, y desarrollar un vocabulario común para discutir la mejor manera de lograr y apoyar esa alineación.

Big data genera una serie cada vez mayor de *círculos concéntricos de influencia*, un complejo de las interacciones y conexiones, que a su vez establece un ecosistema afectado por las implicaciones éticas de cada una de esas interacciones, en tanto que esos nodos generan un conjunto único de circunstancias que incorporan un conjunto de valores y, con ellos, la consideración de las consecuencias sobre dichos valores de las acciones derivadas del uso de los datos.

En este ecosistema, a medida que se utilizan, reutilizan, combinan, correlacionan y procesan determinadas piezas de datos en cada punto de expansión, el impacto de los factores de alineación de valores puede variar considerablemente. Si ya es complejo alinear los valores y la acción de nuestra propia organización, las asociaciones empresariales aumentan la complejidad con cada punto de contacto entre el uso de

los datos que hace la propia organización y el uso que hacen terceros.

Se relacionan a continuación aquellos términos que pueden ser importantes en el momento de acometer un punto de decisión ética:

- Intención. Se refiere a las intenciones finales de aquellos quienes, por medios directos o subrepticios, tienen acceso a los datos.
- Seguridad. Medios que la organización emplea para cumplir los requisitos de seguridad establecidos por la ley o por sus propios cánones de exigencia, que en cualquier caso deben ser más exigentes que aquellos exigidos legalmente.
- Probabilidad. La organización debe establecer la probabilidad real que existe, mediada por las medidas de seguridad adoptadas, de que el acceso a datos específicos resulte en beneficio o daño.
- Agregación. Del mismo modo, la organización debe establecer y hacerse responsable de la combinación de posibilidades derivadas de la correlación de datos disponibles.
- Responsabilidad. Se refiere a los diferentes grados de obligación que surgen en cada punto de la cadena de datos respecto a la consideración de las consecuencias de la acción.
- Identidad. Las colecciones de datos, correlacionados e interrelacionados que permiten que un sujeto sea caracterizado individualmente.
- Propiedad. Trata sobre el estado de la cuestión de quién tiene los derechos de uso en cada punto de la cadena de datos.
- Beneficio. Contribución específica positiva de los datos disponibles a la organización, pero también al usuario.

- Daño. Tipo de daño, sobre la identidad, la privacidad, la intimidad o la reputación, que podría derivarse del acceso a datos específicos.

Cuando se pretende maximizar las operaciones mediante el uso de *big data*, alinear sus valores con sus acciones, también disminuye significativamente el riesgo de consecuencias no deseadas. No eliminará esos riesgos, por supuesto, pero una investigación ética explícita implica que se ha adoptado una metodología legítima para mitigarlos, y a menudo puede proporcionar a las organizaciones un lugar claro para comenzar a trabajar cuando se requiere una respuesta a los muchos interrogantes éticos que la continua e imparable innovación que la tecnología asociada a *big data* genera cada día.

Este capítulo tenía como objetivo la construcción de una estructura mínima, aunque esperemos que sólida, que nos facilite establecer y mantener discusiones éticas en relación con los BD, y no únicamente como profesionales, sino también como clientes, ciudadanos o responsables públicos. Discusiones que nos permitan no solo poner sobre la mesa esos valores que tenemos como personas sino que permitan además a las organizaciones para las que trabajemos tomar decisiones que estén alineadas con su propia cultura, que no es sino el carácter ético de una empresa. Una organización alineada con los valores de las personas que la conforman es, necesariamente, una organización responsable y con ello comprometida con el futuro de la sociedad en la que se inserta.

Bibliografía

Aghazadeh, H. (2017). «Future of Marketology (FOM)». En: *Principles of Marketology, Volume 2* (págs. 391-476). Berlín: Springer.

Agle, B. R.; Mitchell, R. K.; Sonnenfeld, J. A. (2000). «A Report on Stakeholder Attributes and Salience, Corporate Performance and CEO Values». En: J. M. Logsdon; D. J. Wood; L. E. Benson (eds.). *Research in Stakeholder Theory, 1997-1998*. Toronto: The Sloan Foundation Minigrant Project, Clarkson Centre for Business Ethics, University of Toronto.

Bass, B. M.; Avolio, B. J. (1993). «Transformational Leadership and Organizational Culture». En: *Public Administration Quarterly* (págs. 112-121).

Beckhard, R. (1973). *Desarrollo organizacional: estrategias y modelos* (ed. original 1969). México D. F.: Fondo Educativo Interamericano.

Caballero, G.; García, J.; Quintás, M. (2008). «El tiempo y la atención dedicados a los *stakeholders*: un análisis empírico aplicado a la empleabilidad del alumnado de la universidad española». En: *Investigaciones Europeas de Dirección y Economía de la Empresa* (vol. 17, n.º 3, págs. 43-60).

Certo, S. C. (2003). *Modern Management: Adding Digital Focus, Volume 1*. Englewood Cliffs: Prentice Hall.

Cortina, A. (2002). «La dimensión pública de las éticas aplicadas». En: *Revista Iberoamericana de Educación* (vol. 29, n.º 10, págs. 45-64).

Davis, K.; Patterson, D. (2012). *Ethics of Big Data*. Sebastopol: O'Reilly Media Inc.

Donaldson, T.; Preston, L. E. (1995). «The Stakeholder Theory of the Corporation: Concepts, Evidence and Implications». En: *Academy of Management Review* (vol. 20, n.º 1, págs. 65-91).

Etzioni, A. (1998). «A Communitarian Note on Stakeholder Theory». En: *Business Ethics Quarterly* (vol. 8, n.º 4, págs. 679-691).

Freeman, R. E. (1984). *Strategic Management: A Stakeholder Approach*. Boston: Pitman.

Freeman, R. E. (1994). «The Politics of Stakeholder Theory: Some Future Directions». En: *Business Ethics Quarterly* (vol. 4, n.º 4, págs. 409-421).

García-Crespo, Á.; Ceballos, M.; González-Carrasco, I.; Lado, N.; López-Cuadrado, J. L. (2017). «Innovation in the Spanish Twittersphere: An Ontology and Stakeholders' Salience Analysis». En: *Revolution of Innovation Management* (págs. 97-128). Berlín: Springer.

González Esteban, E. (2007). «La teoría de los stakeholders. Un puente para el desarrollo práctico de la ética empresarial y de la responsabilidad social corporativa». En: *Veritas* (vol. 2, n.º 17, págs. 205-224).

McAdam, D.; Scott, R. W. (2005). «Organizations and Movements». En: G. F. Davies; D. McAdam; R. W. Scott; M. N. Zald (eds.). *Social Movements and Organization Theory* (págs. 4-40). Cambridge: Cambridge University Press.

McAfee, A.; Brynjolfsson, E. et al. (2012). «Big Data: The Management Revolution». En: *Harvard Business Review* (vol. 90, n.º 10, págs. 60-68).

Mitchell, R. K.; Agle, B. R.; Wood, D. J. (1997). «Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts». En: *Academy of Management Review* (vol. 22, n.º 4, págs. 853-886).

Phillips, R. A.; Freeman, R. E.; Wicks, A. C. (2003). «What Stakeholder Theory is Not». En: *Business Ethics Quarterly* (vol. 13, n.º 4, págs. 479-502).

Pool, S. W. (2000). «The Learning Organization: Motivating Employees by Integrating TQM Philosophy in a Supportive Organizational Culture». En: *Leadership & Organization Development Journal* (vol. 21, n.º 8, págs. 373-378).

Pop, N. A.; Dabija, D. C.; Iorga, A. M. (2017). «Ethical Considerations Regarding Stakeholders in Neuromarketing Research. Empirical Insights from NMSBA Corporate Members, TAAN Advertising Agencies and Romanian Companies». En: *Ethics and Neuromarketing* (págs. 123-146). Berlín: Springer.

Ramdhani, A.; Ramdhani, M. A.; Ainisyifa, H. (2017). «Conceptual Framework of Corporate Culture Influenced on Employees Commitment to Organization». En: *International Business Management* (vol. 11, n.º 3, págs. 826-803).

Rawls, J. (1971). *A Theory of Justice*. Massachussets: Harvard University Press.

Richards, N. M. (2014). «Four Privacy Myths». En: A. Serat (ed.). *A World Without Privacy: What Law Can and Should Do?* (págs. 33-82). Cambridge: Cambridge University Press.

Saz Gil, M.a I. (2008). «Introducción a la gestión Stakeholder en las organizaciones no lucrativas. Una aproximación a través del estudio de casos». En: *Estudios de Economía Aplicada* (vol. 26, n.º 1, págs. 187-210).

Shenkar, O.; Yuchtman Yaar, E. (1997). «Reputation, Image, Prestige and Goodwill: An Interdisciplinary Approach to Organizational Standing». En: *Human Relations* (vol. 50, n.º 11, págs. 1.361-1.381).

Tseng, M. L.; Chiu, A. S.; Liang, D. (2017). *Sustainable Consumption and Production in Business Decision-Making Models*. Ámsterdam: Elsevier.

Tuleja, T. (1987). *Más allá de la cuenta de resultados*. Barcelona: Plaza&Janés.

Wartick, S. L.; Wood, D. J. (2000). *International Business and Society*. Malden: Blackwell Publishing Ltd.

Wisniewski, M.; Stewart, D. (2004). «Performance Measurement for Stakeholders: The Case of Scottish Local Authorities». En: *International Journal of Public Sector Management* (vol. 17, n.º 3, págs. 222-233).

Wood, D. J.; Jones, R. E. (1995). «Stakeholder Mismatching: A Theoretical Problem in Empirical Research on Corporate Social Performance». En: *Journal of Organizational Analysis* (vol. 3, n.º 3, págs. 229-267).

Capítulo V

La regulación de los sistemas de *big data* e inteligencia artificial

1. Introducción

La inteligencia artificial (AI, por sus siglas en inglés) ya no es solo uno de los temas favoritos de las novelas de ciencia ficción, sino que se ha ido incorporando paulatinamente a nuestra forma de vida de un modo que podríamos considerar prácticamente definitivo. Las razones que nos permiten mantener esta afirmación las hemos venido desarrollando en los anteriores capítulos, y se concretan en: i) la transformación de los sistemas de información en una red cada vez más extensa de aparatos electrónicos inteligentes interconectados, lo que hemos llamado aquí IoT; ii) la disponibilidad de cantidades masivas de datos, *big data*; iii) la accesibilidad a servidores que facilitan el registro y almacenamiento barato de cantidades de datos que crecen exponencialmente; y iv) el desarrollo de métodos estadísticos y de aprendizaje automático cada vez más sofisticados, que pretenden extraer conocimiento de estas colecciones de datos desestructurados.

Estos cuatro puntos se refuerzan entre ellos y evidencian la viabilidad, importancia y escalabilidad que la AI irá tomando progresivamente en la organización social y política. Efectivamente, los BD tienen un potencial sin precedentes en lo que respecta a almacenar, combinar,

analizar y visualizar conjuntos de datos, y ello hace que tengan capacidad para revelar aspectos del comportamiento y procesos humanos que antes eran difíciles, si no imposibles, de determinar. Por esto, se espera que muy pronto sea posible incorporar un nuevo punto a esa lista en el que se indique ya no solo la preocupación o la llamada de atención sobre la necesaria incorporación de la ética a esta actividad, sino la constatación de dicha incorporación, ya sea mediante el diseño de políticas adecuadas que permitan dirimir las responsabilidades, códigos éticos adoptados por empresas y profesionales, o tribunales que pretendan la justicia y no la mera persecución de los incumplimientos de unas normas que se verán siempre superadas por la velocidad a la que operan las innovaciones y los riesgos en este escenario.

Un análisis, desde la ética, que pretenda confrontar la gestión de la responsabilidad en el escenario que conforman BD, la IoT y la IA, debe considerar cuestiones basadas en el *para qué* y el *hacia dónde*, en vez de, como es habitual en tecnología, únicamente aquellas que se refieren al *cómo*. Cuestiones como *dónde queremos llegar*, o bien, *cuáles son nuestros objetivos como humanidad* implican necesariamente un discurso orientado hacia el bien común, hacia una sociedad justa, una sociedad inclusiva y democrática. La buena noticia es que hace años que existe un consenso sobre cómo debe ser ese futuro que queremos. *Our Common Future* fue el informe de Naciones Unidas, liderado por Gudrun Brundtland y aprobado en su Asamblea General en 1985. Este informe recoge los primeros objetivos comunes de desarrollo consensuados mundialmente. Ese desarrollo fue bautizado como *sostenible* y una de sus principales y

novedosas características es que, para denominarse sostenible, cualquier forma de desarrollo debería contemplar necesariamente su impacto sobre las generaciones futuras (World Commission on Environment and Development, 1987). Los *Objetivos de desarrollo del milenio* (ODM) fueron adoptados en 2000 por los 189 países de los que componen la Asamblea General. Finalmente, en 2015, fueron aprobados también en Asamblea General los *Objetivos de desarrollo sostenible* (ODS).[1] Los ODS comprenden 17 objetivos y 169 metas con las que se pretenden erradicar la pobreza, combatir las desigualdades y promover la prosperidad y desarrollo de los pueblos, al tiempo que se protege el medio ambiente y se combate el cambio climático. Hay una cuestión adicional que se refiere a cómo hacer efectiva la incorporación de los ODS a las políticas de responsabilidad social de la empresa (RSE) y cómo evidenciar que el cumplimiento de estos objetivos contribuye a conformar una cultura ética empresarial, paso previo ineludible para desarrollar unas políticas de responsabilidad verosímiles y que dispongan, ahora sí, de suficiente potencia como para incrementar la credibilidad y reputación de las empresas.

Sin embargo, parece que el escenario, o ambiente, que resulta de la interacción de las personas con los sistemas de información, y que algunos denominan *infosfera*, vive ajena a los objetivos que deseamos como humanidad para la *bioesfera*. Paradójicamente, en las sociedades de la información maduras

1 ONU (2015). Proyecto de documento final de la cumbre de las Naciones Unidas para la aprobación de la agenda para el desarrollo después de 2015 (seguimiento de los resultados de la Cumbre del Milenio n.º A/69/L.85). Nueva York. Cfr. <http://www.un.org/sustainabledevelopment>

(*mature information societies*) cuanto más normalizada está la aplicación y el uso de la AI, más dificultades encuentran las personas para saber cómo funcionan realmente esas interconexiones y redes, cómo afectan a nuestra organización social y a los valores cívicos y éticos que conforman estructuralmente la sociedad (Floridi, 2016). Lo que viene a mostrar que a pesar de que estemos incrementando sucesivamente nuestras conexiones, el acceso a la información y se dispongan de más medios inteligentes, nuestra capacidad para responder a aquella pregunta que apuntaba hacia el *para qué* se verá proporcionalmente limitada. Por esto, precisamente, es urgente la articulación de iniciativas que vinculen los deseos expresados por la asamblea de Naciones Unidas por un mundo mejor, con las capacidades de la AI, desde dentro, por empresas y profesionales, desde los gobiernos e instituciones públicas, e incorporando a actores de la sociedad civil. Para lograr este objetivo es que necesitaremos un enfoque multi-*stakeholder*, adaptado a la complejidad del problema abordado, al que aludimos en el capítulo 3.

En este capítulo se presentarán las iniciativas para atender estos requerimientos desarrolladas por algunos de los grupos de interés reconocidos, aunque obviamente, identificar y analizar a todos ellos supondría una tarea que supera en mucho el objetivo de este capítulo y de este libro. Se presentarán entonces las aproximaciones al problema realizadas desde la Executive Office of the President, en diciembre de 2016; desde el European Parliament's Committee on Legal Affairs, en febrero de 2017; desde la Association for Computing Machinery, actualmente en proceso de renovación de su código ético, previsto para enero de 2018; y desde la sociedad civil, en particular, el papel que los *hackers*-buenos están representando en la observancia de principios y valores éticos.

2. Preparando las sociedades para el futuro: propuestas desde Estados Unidos

El informe *Artificial Intelligence, Automation, and the Economy*, realizado para la Executive Office of the President (EOP), en diciembre de 2016,[2] está basado en *workshops* y grupos expertos de discusión previos, realizados bajo el lema «Preparing for the Future of Artificial Intelligence», y organizados por la White House Office of Science and Technology Policy (OSTP) y el National Science and Technology Council (NSTC) desde mayo de 2016 y que concluiría con la redacción de un informe en octubre de ese mismo año.[3]

El informe reconoce la importancia que tendrá la AI en el desarrollo futuro de la inteligencia humana, pero parece considerar la AI como un fenómeno ajeno e independiente de la propia inteligencia de los seres humanos: «Desarrollar y estudiar la inteligencia de las máquinas puede ayudar a comprender y apreciar mejor nuestra inteligencia humana».[4] De hecho, la metáfora que utiliza el presidente Obama en una entrevista para referirse a la AI, aludiendo al proceso de floración primaveral, implica reconocer que estamos ante

2 Versión en PDF disponible en: <https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF>

3 Versión en PDF disponible en: <https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf>. Una revisión del proceso de redacción del informe, está disponible aquí: <https://obamawhitehouse.archives.gov/blog/2016/05/03/preparing-future-artificial-intelligence>

4 La traducción es nuestra. El texto original dice: «Developing and studying machine intelligence can help us better understand and appreciate our human intelligence. Used thoughtfully, AI can augment our intelligence, helping us chart a better and wiser path forward» (OSTP, 2016, págs. 14, 49).

una innovación en la que apenas se puede, y debe, intervenir: «La forma en la que he estado pensando sobre la estructura reguladora de la AI es que tratándose de una tecnología que apenas comienza, y en la que *miles de flores deben aún florecer* […] el gobierno debería aportar apenas un ligero toque, haciendo una inversión fuerte en investigación y asegurándose de que hay una conversación entre la investigación base y la investigación aplicada».[5]

Esta conversación alude significativamente a la necesaria e imprescindible colaboración entre el gobierno y las empresas, aunque el sentido de esa colaboración implica la habitual «poca o nula» intervención del gobierno estadounidense en la regulación de aquellos sectores de la economía que están liderando la innovación en el uso de la AI: finanzas, armamento, automoción, aviación y telecomunicaciones. La colaboración será entendida, esencialmente, en términos de investigación y no solo para seguir de cerca el desarrollo de la AI, sino para «asegurarse de que la comunidad científica concentra esfuerzos en asegurar que la AI sea responsable, transparente y sus operaciones son coherentes con los valores y las aspiraciones humanas».[6]

Aunque el informe asegura que la AI es una tecnología que, utilizada con cautela, puede ayudar a aumentar las capacidades humanas más que a reemplazarlas, uno de los temas

5 La traducción es nuestra. El texto original puede encontrarse en: <https://www.wired.com/2016/10/obama-envisions-ai-new-apollo-program>

6 La traducción es nuestra. El texto original dice: «The report emphasizes the importance of research. Not only in order to monitor on-going developments in AI, but also to ask the research community to focus its efforts on ensuring that AI is accountable, transparent, and [its] operation will remain consistent with human values and aspirations» (OSTP, 2016, pág. 4).

en los que se detiene es en el efecto que va a tener la AI en el mercado de trabajo y este es precisamente el asunto que da pie al informe inmediatamente posterior: *Artificial Intelligence, Automation, and the Economy*, de diciembre de 2016. De hecho, toman como hipótesis que los trabajadores de salarios bajos y medianos tienen más probabilidades de ser afectados negativamente por la AI, y que el gobierno debe desarrollar políticas públicas para asegurar que la AI no aumenta la desigualdad económica. Así, de las tres líneas políticas que se adoptan en el informe, dos hacen referencia explícita a cómo va a afectar la AI a los trabajadores (EOP, 2016, pág. 27).

Las pretensiones de estos documentos son loables, aunque poco realistas con su capacidad de incidencia en la industria que pretenden afectar.[7] Por ejemplo, a pesar de que el informe reconoce los dilemas éticos a los que se enfrenta la aplicación de IA en el denominado *armamento autónomo* (*lethal autonomous weapons* —LAWs), afirmar que las agencias del Gobierno de los Estados Unidos «están trabajando de acuerdo con la legislación humanitaria internacional sobre el uso de los LAWs»,[8] no parece el modo más adecuado de confrontar esos dilemas, sino más bien un modo de obviarlos. Efectivamente, no parece posible confrontar de un modo efectivo los problemas que se generan por una tecnología no solo absolutamente nueva,

7 Véase, por ejemplo, «Drones and Aerial Surveillance: Considerations for Legislatures», Gregory McNeal, *The Brookings Institution*: <https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures>

8 La traducción es nuestra. El texto original dice: «Agencies across the U.S. Government are working to develop a single, government-wide policy, consistent with international humanitarian law, on autonomous and semiautonomous weapons» (EOP, 2016, pág. 3).

sino que se rehace de forma constante, con herramientas legales del siglo XX (Taddeo, 2016).

Aunque las descripciones de los problemas son precisas, incidiendo mucho más en las oportunidades y ventajas que en los riesgos, no llegan a establecer un diseño sociopolítico suficientemente comprehensivo. Así, especialmente el primero de los documentos ha sido considerado no más que «un interesante esquema de objetivos de investigación» (Cath *et al.*, 2017, pág. 6).

3. Regulación de algoritmos y robots: propuestas desde la UE

El Parlamento Europeo aprobó la Resolución del Parlamento Europeo, del 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre Normas de Derecho Civil sobre Robótica (2015/2103 [INL]).[9] El informe previo había sido preparado por la Comisión de Asuntos Jurídicos (JURI), y las opiniones de miembros de la Comisión de Industria, Investigación y Energía (ITRE), de la Comisión de Mercado Interior y Protección del Consumidor (IMCO) y de la Comisión de Empleo y Asuntos Sociales (EMPL).

En su introducción se enumeran veinte consideraciones, la primera de ella aludiendo a lo inminente de una nueva revolución industrial desencadenada precisamente por «robots, bots,

9 Resolución del Parlamento Europeo, del 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre Normas de Derecho Civil sobre Robótica (2015/2103 [INL]): <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//ES>

androides y otras formas de inteligencia artificial cada vez más sofisticadas»[10] que afectará a todos los estratos de la sociedad y que ello justifica que el legislador pondere las consecuencias jurídicas y éticas. Para ello, se considera a continuación la necesidad de establecer una definición generalmente aceptada de robot y de inteligencia artificial que sea flexible y no lastre la innovación, y así se hace en el más adelante: «Debe establecerse una definición europea común de robots autónomos "inteligentes", cuando proceda, incluidas las definiciones de sus subcategorías, teniendo en cuenta las siguientes características: la capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el análisis de dichos datos; la capacidad de aprender a través de la experiencia y la interacción; la forma del soporte físico del robot; la capacidad de adaptar su comportamiento y acciones al entorno» (Delvaux, 2017, pág. 9).[11]

Los efectos positivos de la irrupción de los robots se establecen primero en términos económicos, para incidir después en la eficiencia, ahorro y seguridad y mejora de la calidad de los servicios que su uso está provocando en el funcionamiento, progreso y organización de las sociedades.[12] Sin embargo, también se apunta a los riesgos y los efectos negativos que estos pueden tener en la seguridad de las personas, sobre la desigualdad, la inequidad y su incidencia en el mercado de

10 La norma europea se ocupa específicamente de «vehículos autónomos, incluidos los drones, y robots de uso asistencial y médico» (Delvaux, 2017, págs. 13-16). Nos referiremos a todas ellas de ahora en adelante únicamente con el término *robot*.

11 De aquí en adelante todas las referencias a esta resolución se harán indicando únicamente el número de página.

12 Consideraciones D-F (págs. 3-4).

trabajo, y en la necesidad de adoptar una serie de normas en materia de responsabilidad, transparencia y rendición de cuentas que reflejen los valores humanistas intrínsecamente europeos y universales, incidiendo insistentemente en que no se pretende en ningún caso obstaculizar la innovación.[13]

Sobre *responsabilidad* se hacen diez consideraciones, de la que queremos resaltar el reconocimiento de que «la autonomía de los robots suscita la cuestión de su naturaleza y de si pertenecen a una de las categorías jurídicas existentes o si debe crearse una nueva categoría con sus propias características jurídicas» (pág. 7), que vendría a reconocer la necesidad urgente de identificar a ese nuevo sujeto moral que opera en el escenario de BD al que nos referíamos en el capítulo 1, haciéndose manifiestas las deficiencias del marco jurídico vigente.[14] A resaltar la relación entre innovación e investigación, así como la integración de ambas en la economía, se dedican seis puntos de los principios generales, pidiendo específicamente «a la Comisión y a los Estados miembros que aúnen sus esfuerzos para supervisar detenidamente la transición de estas tecnologías de la investigación a la comercialización y el uso en el mercado y para garantizar que esta transición se produzca de forma fluida, tras las oportunas evaluaciones de su seguridad con arreglo al principio de precaución» (pág. 10).

Se subraya la importancia de evaluar los riesgos «a la luz de la seguridad y la salud humanas; la libertad, la intimidad, la integridad y la dignidad; la autodeterminación y la no discriminación, y la protección de los datos personales» (pág. 10). El marco de orientaciones éticas que permitirán salvaguardar

13 Consideraciones G-X (págs. 4-6).

14 Consideraciones sobre responsabilidad: AG-AI (pág. 8).

estos valores serán los principios de beneficencia, autonomía, justicia y no-maleficencia, a los que aludimos en este trabajo en su capítulo 2, y «en los principios consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, así como en otros principios y valores inherentes al Derecho de la Unión, sin olvidar las actuales prácticas y códigos éticos» (pág. 11).

Se incide igualmente en la necesidad de observar y reforzar las leyes de protección de datos, en especial en aquello que pueda afectar a la intimidad y privacidad de las personas. En este sentido, se está desarrollando un nuevo Reglamento General de Protección de Datos, cuya entrada en vigor como ley en toda la UE se estima para 2018. Con ella, se pretende restringir la toma de decisiones individual automatizada, es decir, los algoritmos que toman decisiones basadas en predictores a nivel de usuario que «afectan significativamente» a los usuarios. La ley también regulará lo que se denomina el *derecho a una explicación*, por el que un usuario puede pedir una explicación de una decisión algorítmica que se hizo sobre ellos. Esta ley planteará grandes desafíos para la industria, pero es una oportunidad para que los científicos de la computación tomen la iniciativa en el diseño de algoritmos y marcos de evaluación que eviten la discriminación y la explicación de sus algoritmos mediante la adopción de criterios de transparencia (Goodman; Flaxman, 2016).

4. Código de ética y conducta profesional de la Association for Computing Machinery

La Association for Computing Machinery (ACM), una sociedad con más de cien mil miembros en todo el mundo,

está procediendo a la renovación participada de su Código de ética y conducta profesional, un código que fue modificado por última vez en 1992.[15] Se trata de un proceso que comenzó en abril de 2017, con la exposición pública abierta de un primer borrador, al que se podrán realizar enmiendas y aportaciones hasta el 5 de junio de 2017. Un segundo borrador será presentado entonces a la comunidad para recibir nuevas aportaciones. Se espera disponer de un código aprobado para la primavera de 2018.[16]

El equipo que ha realizado los diferentes borradores, y está llamado a aprobar el documento definitivo, está conformado por 37 miembros, de los cuales: 6 pertenecen al comité que coordina; 4 son representantes de la industria (2 de Google, 1 de Microsoft y 1 de Intel); 4 representantes de otras asociaciones y sociedades profesionales (1 del Reino Unido, 1 de Finlandia, 1 de Alemania y 1 de China); 12 miembros de ACM; 5 especialistas independientes; y 6 son miembros del Comité de Ética de ACM.

El nuevo código debe enfrentar en primer lugar los significativos cambios que han operado desde 1992, en particular, aquellos que se refieren específicamente a la rápida progresión de la tecnología de la computación; aquellos que se refieren a cómo la tecnología se ha integrado en la vida cotidiana de las personas y en las estructuras sociales; y, finalmente, al número y tipos de grupos de interés (*stakeholders*) que se ven afectados por las tecnologías de la computación. Así, aunque

15 «1992 ACM Code of Ethics and Professional Conduct. Adopted by the ACM Council 1992-10-16»: <https://ethics.acm.org/code-of-ethics/previous-versions/1992-acm-code>

16 La relación completa de documentos que conforman el proceso, puede consultarse en «Code 2018 Project»: <https://ethics.acm.org>

en el código de 1992 se estableciese que la actividad de los profesionales de la computación «debía contribuir al bienestar del ser humano y de la sociedad» (Code 92, 1.1), se reconoce que los profesionales «han estado más ocupados en atender la complejidad técnica de la computación, que las implicaciones éticas de su propia actividad» (Gotterbarn, 2016, pág. 35). Por eso este nuevo código pretende trascender la mera relación de compromisos éticos que suelen conformar los códigos éticos, y que suelen pasar a ser bien un anexo a un libro que nadie lee, o la pestaña de una página web a la que nadie accede. Por esto, precisamente, es tan interesante la propuesta «participada» del nuevo código ético que promueve la ACM: «Pretendemos desarrollar nuevos medios para promover la integridad en la profesión. No podemos hacerlo solos, y estamos pidiendo a los miembros del SIGCAS que se ofrezcan voluntariamente y se involucren» (Brinkman *et al.*, 2016, pág. 5).

Las principales aportaciones del Código 2018, se pretende que sean las siguientes:

- La necesidad de que los profesionales de la computación comprendan mejor cómo la tecnología y sus artefactos impactan en las personas y en la infraestructura social, y que su objetivo final debe ser, en cualquier caso, la promoción del «bien común».[17] La condición de profesionales en computación exige «mejorar nuestras capacidades para

17 Tanto en estos documentos como en los analizados en el epígrafe 5.2 de este capítulo, se utilizan indistintamente los términos *public good* y *common good* para referirse a aquello que nosotros denominamos en este libro *bien común*, y que quedó definido en el capítulo 1.

anticipar impactos en el más amplio espectro, positivos y negativos, y asumir la responsabilidad por esos impactos.»

- El término *profesional de la computación* incluye: estudiantes e ingenieros/as de software, arquitectos/as de software, CEOs, profesores e investigadores.
- El Código 2018 pretende proporcionar herramientas que permitan orientar a la comunidad involucrada en la toma de decisiones. Sustituyendo el lenguaje categórico de *imperativos morales*, por uno prescriptivo de *principios éticos*. Cada uno de los principios recogidos en el Código debe ayudarnos a entender nuestra responsabilidad ética y guiar nuestra toma de decisiones en contextos variables y situaciones, en lugar de proporcionar un sistema de reglas o normas, a acatar, sin pensar en las consecuencias.
- El Código 2018 pretende ser de aplicación a profesionales de la computación de todo el mundo, independientemente de su afiliación con el ACM. En cualquier caso, los miembros de ACM asumen la responsabilidad adicional de fomentar y apoyar la adhesión al Código 2018 por todos los profesionales con los que se relacionen. Además, los miembros de la ACM que violen el Código 2018 verán cancelada su pertenencia a la sociedad (Wolf, 2016, págs. 105-106).

5. La sociedad civil: *hackers*, ONG

En este repaso sobre las iniciativas que se están llevando actualmente para la regulación de aquellas actividades relacionadas con BD, no era posible dejar de mencionar el papel que la sociedad civil ha representado en la regulación

de todas aquellas áreas en las que la innovación ha supuesto un reto a la ética; nos referimos a los alimentos transgénicos, el ensayo y comercialización de nuevos medicamentos o la nanotecnología; en todas ellas, el papel de los denominados *whistleblowers*, aquellos quienes hacen uso de la *denuncia pública* llaman la atención sobre algún tipo de injusticia o abuso de poder (VV. AA., 2011).

Los *whistleblowers*, o centinelas, si adoptamos el término que se emplea en biología para señalar a aquellas especies que ejercen el papel de alertar de un peligro inminente, bien porque son más vulnerables que otras, como las abejas, bien porque están mejor organizadas como comunidad y deciden movilizarse hacia un lugar seguro, horas o días antes de que una catástrofe ocurra. Los *centinelas* pueden estar organizados, en una ONG, como Greenpeace,[18] o en una asociación no reconocida legalmente, como Wikileaks.[19] También hay centinelas que han actuado de modo individual, denunciando temas concretos, como el ingeniero de sistemas Hervé Falciani, quien denunció ante las autoridades de varios países europeos en 2008, a un total de 130.000 evasores fiscales;[20] o Edward Snowden, de quien ya hemos hablado aquí, quien denunció los programas de vigilancia masiva llevados a cabo desde agencias estatales estadounidenses.

18 Desde 2009, Greenpeace International mantiene la campaña Cool IT Challenge con objeto de llamar la atención sobre los compromisos que la industria tecnológica debe asumir para frenar el cambio climático: <http://www.greenpeace.org/international/en/campaigns/climate-change/cool-it>

19 Desde noviembre de 2010, la organización global y sin ánimo de lucro, liderada por Julian Assange, desvela secretos de gobiernos y empresas a través de su página web: <https://wikileaks.org>

20 Ver documental del canal ARTE sobre Swiss Leaks o caso Falciani: <http://falciani-info.arte.tv/?lang=es#/chapter/1>

Por otro lado, el término *hacker* se utiliza desde los años cuarenta y cincuenta para designar a aquellas personas con habilidades para «acceder» a un sistema sin haber sido invitados. Las intenciones que tenga la persona para acceder al sistema son fundamentales para denominarle *hacker*, si estas intenciones son beneficiosas, o *cracker*, si las intenciones son maliciosas. También se denominan *white-hat* a los primeros, y *black-hat* a los segundos (Holt; Schell, 2013). En cualquier caso, establecer qué es lo bueno y qué es lo malo para los sistemas, llevaría a un estudio detallado de guerra de intereses, que puede ser política, económica o ambas, que excede en mucho el objeto de este trabajo.[21]

Lo que es evidente es que la denominada ética *hacker* tiene unos valores que están muy relacionados con la incorporación de las tecnologías en la vida cotidiana, y en particular en la educación. Por ello, no debe extrañar que tanto en escuelas secundarias (Niiler, 2013), como en las universidades (Curbelo; Cruz, 2013), se promuevan cursos de programación que permitan desarrollar habilidades para llegar un *hacker*-bueno, que en la sociedad contemporánea vendría a ser lo mismo que en las sociedades anteriores un simple buen-ciudadano.

21 Véase, por ejemplo, la conexión entre la intervención rusa a través de ¿*hackers* o *crackers*? en la campaña para la presidencia de los Estados Unidos de Donald Trump, aún bajo investigación: «Russia: The Scandal Trump Can't Shake», *BBC News*, 17 de mayo de 2017: <http://www.bbc.com/news/world-us-canada-38966846>

Bibliografía

Brinkman, B.; Gotterbarn, D.; Miller, K. W.; Wolf, M. J. (2016). «All Hands on Deck for ACM Ethics: Updating the Code, Revising Enforcement, Promoting Integrity». En: *SIGCAS Comput. Soc.* (vol. 46, n.º 3, págs. 5-8).

Cath, C.; Wachter, S.; Mittelstadt, B.; Taddeo, M.; Floridi, L. (2017). «Artificial Intelligence and the "Good Society": The US, EU, and UK Approach». En: *Science Engineering Ethics* (págs 1-24).

Curbelo, A. M.; Cruz, A. (2013). «Faculty Attitudes toward Teaching Ethical Hacking to Computer and Information Systems Undergraduates Students» [informe de investigación en línea]. En: *Proceedings of the Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology*. [Fecha de consulta: 28 de junio de 2017]. <http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP086.pdf>

Delvaux, M. (2017). *Normas de derecho civil sobre robótica.* Resolución del Parlamento Europeo, del 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre Normas de Derecho Civil sobre Robótica (n.º 2015/2103 [INL]) [informe en línea]. Bruselas: Parlamento Europeo.

Executive Office of the President (2016). *Artificial Intelligence, Automation, and the Economy* [informe en línea]. Washington: White House. [Fecha de consulta: 2 de junio de 2017]. <https://obamawhitehouse.archives.gov/blog/2016/12/20/artificial-intelligence-automation-and-economy>

Floridi, L. (2016). «Mature Information Societies—a Matter of Expectations». En: *Philosophy & Technology* (vol. 29, n.º 1, págs. 1-4).

Goodman, B.; Flaxman, S. (2016). «European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"» [informe en línea]. En: *arXiv Preprint arXiv:1606.08813*. [Fecha de consulta: 7 de junio de 2017]. <https://arxiv.org/pdf/1606.08813.pdf>

Gotterbarn, D. (2016). «Thinking Professionally: Codes of Ethics—: The Conscience of a Profession: Connecting Technology and Society». En: *ACM Inroads* (vol. 7, n.º 4, págs. 33-35).

Holt, T. J.; Schell, B. H. (2013). *Hackers and Hacking: A Reference Handbook*. Santa Bárbara: ABC-CLIO.

Niiler, E. (2013). «Cyber warriors. Teens develop "ethical hacking" skills to defend computer systems» [artículo en línea]. En: *Science News for Students*. [Fecha de consulta: 12 de junio de 2017]. <https://www.sciencenewsforstudents.org/article/cyber-warriors>

Office of Science and Technology Policy (2016). *Preparing for the Future of Artificial Intelligence*. Washington: White House.

Taddeo, M. (2016). «Just Information Warfare». En: *Topoi* (vol. 35, n.º 1, págs. 213-224).

Wiener, J. B.; Rogers, M. D.; Hammitt, J. K.; Sand, P. H. (eds.) (2011). *The Reality of Precaution. Comparing Risk Regulation in the United States and Europe*. Washington: RFF Press.

World Commission on Environment and Development (1987). *Our Common Future*. G. H. Brundtland (coord.). Madrid: Alianza.

ROSA COLMENAREJO FERNÁNDEZ

TECNOLOGÍA

UNA ÉTICA PARA BIG DATA

INTRODUCCIÓN A LA GESTIÓN ÉTICA DE DATOS MASIVOS

Este libro trata sobre cómo la ética afecta, y se ve afectada, por el cambiante e inasible mundo de los datos. Sirviéndose de voces autorizadas por la academia, de asociaciones profesionales y de instituciones públicas, norteamericanas y europeas, la autora perfila el escenario que emerge del uso de la internet de las cosas para la obtención de datos masivos; identifica los principales problemas que atañen a su almacenamiento, procesamiento y utilización; y aporta sugerencias sobre cómo puede contribuir la ética a gestionar estos procesos de un modo orientado hacia el bien común.

Con este libro aprenderás sobre:

✓ ética; ✓ *big data*; ✓ internet de las cosas; ✓ responsabilidad; ✓ *computer ethics*; ✓ *internet ethics*; ✓ *bioethics*; ✓ deontología; ✓ consecuencialismo; ✓ principios profesionales; ✓ autonomía; ✓ justicia; ✓ privacidad; ✓ identidad digital; ✓ reputación digital; ✓ toma de decisiones; ✓ regulación; ✓ códigos éticos

Rosa Colmenarejo Fernández

Doctora por la Universidad de Córdoba, su principal línea de investigación está centrada en la caracterización de una ética de la emancipación, a partir del desarrollo de capacidades que facilitan la cultura y la tecnología.

EDITORIAL UOC