

---

# Ética y *big data*

---

PID\_00243550

Rosa Colmenarejo Fernández

---

Tiempo mínimo de dedicación recomendado: 4 horas

---





# Índice

<b>Introducción.....</b>	<b>5</b>
<b>Objetivos.....</b>	<b>8</b>
<b>1. Ética y <i>big data</i>.....</b>	<b>9</b>
1.1. Introducción .....	9
1.2. ¿Dónde ubicar una ética de los <i>big data</i> ? .....	11
1.3. El problema del sujeto moral .....	12
1.3.1. Ética y moral: caracterización del sujeto moral precomputacional .....	12
1.3.2. ¿Un giro copernicano para la ética de los <i>big data</i> ? .....	15
1.4. Conclusiones del apartado 1 .....	15
<b>2. ¿Qué debo hacer? ¿Lo bueno, lo justo o lo correcto?</b>	
<b>Teorías éticas y principios profesionales.....</b>	<b>17</b>
2.1. Introducción .....	17
2.2. Teorías éticas. Breve introducción .....	18
2.3. Principios orientadores de la acción del buen profesional .....	20
2.3.1. Principio de beneficencia .....	21
2.3.2. Principio de autonomía .....	22
2.3.3. Principio de no maleficencia .....	24
2.3.4. Principio de justicia .....	26
2.4. Conclusiones del apartado 2 .....	26
<b>3. Conceptos fundamentales para una ética aplicada a <i>big data</i>.....</b>	<b>28</b>
3.1. Introducción .....	28
3.2. Identidad .....	28
3.2.1. Una dirección IP no da cuenta de nuestra identidad ....	29
3.2.2. La identidad se moldea en el tiempo y en el espacio- red .....	30
3.3. Privacidad .....	31
3.3.1. Privacidad <i>offline</i> frente a <i>online</i> .....	32
3.3.2. Problemas de privacidad generados por <i>big data</i> .....	33
3.3.3. Hacia una gestión de la privacidad justa y equitativa: entre la ética y la ley .....	35
3.4. Propiedad y pertenencia .....	39
3.5. Reputación .....	40
3.6. Conclusiones del apartado 3 .....	41
<b>4. La toma de decisiones éticas.....</b>	<b>42</b>

4.1. Introducción .....	42
4.2. Puntos de decisión ética .....	44
<b>5. Conclusiones finales.....</b>	<b>48</b>
<b>Bibliografía.....</b>	<b>49</b>

## Introducción

Lo que denominamos *Internet de las cosas* (IoT, por sus siglas en inglés) está conformando un nuevo escenario en el que todas y cada una de las personas que disponemos de un teléfono móvil, un reloj inteligente o interaccionamos con dispositivos electrónicos sensibles, ya sea en el gimnasio, en la consulta médica o en el hipermercado, estamos suministrando “datos” de forma simultánea y continua, a la velocidad que nos permita la conexión, datos que son además fiables y aportados de forma voluntaria, aunque no siempre de acuerdo con suficiente información respecto al consentimiento que damos para su utilización por parte de terceros.

Aunque se habla mucho de *big data* y de IoT como si fuesen la misma cosa, y muchos lo señalan como una “moda” que será necesariamente pasajera, la realidad es que esta forma de generar datos ha llegado para quedarse y crecer. Google nos ofrecía allá por 2003 algunas cifras que parece interesante recordar aquí para no perder de vista la magnitud de lo que *big data* se trae entre manos: si hasta ese mismo año la humanidad había generado, a lo largo de su historia, un total de 5 exabites de datos fue entonces cuando se comenzaron a producir esos 5 exabites ¡cada dos días! Las previsiones apuntaban entonces a que en 2016 los datos generados se habrán multiplicado por cuatro. Parece que la humanidad hubiese encontrado, al fin, un recurso aparentemente infinito para explotar. No olvidemos que 1 exabite es 10 elevado a 17. Aunque, en realidad, no es tanto la cantidad como la naturaleza, desestructurada y liberada al fin de las filas y columnas que han soportado las colecciones tradicionales de datos, lo que caracteriza la potencia de lo que ahora denominamos *big data*.

Esta forma de generar, almacenar y procesar datos está transformando la comunicación, pero también la sociedad misma. El *time line* de una cuenta de Twitter que se ocupa de compartir toda información etiquetada como #Big-Data, se hace eco, principalmente, de la amabilidad y ventajas que ofrece ese escenario en el que se confía a la IoT la conformación de un mundo pretendidamente “mejorado”. Más eficiente, más seguro, más transparente. Así, *big data* se está convirtiendo en el término mágico al que aludir para pensar en el futuro: mejorar la eficiencia de los procesos de negocio, la toma de decisiones en investigaciones biomédicas que deben atender casos complejos que se mueven en más de 50 o 60 dimensiones, como es el caso de las asignaciones de órganos en trasplantes, la gestión del tráfico o de las inversiones. Los proyectos de “ciudades inteligentes” son un buen ejemplo, la comunidad gana, las empresas ganan y las instituciones ganan. ¿Todos ganan? La pregunta fundamental aquí es ¿para qué? ¿Cuál es la finalidad que persiguen cada uno de estos grupos que generan, almacenan, procesan, gestionan y, finalmente, utilizan ese conocimiento? ¿Tienen los mismos intereses?

La realidad es que las redes sociales, las aplicaciones de mensajería instantánea o las de geolocalización nos fueron ofrecidas como inocentes juegos que hemos adaptado a nuestra vida cotidiana con la ilusión de estar mejor informados y conectados, tanto en la esfera personal como profesional. Algunos incluso parece que fueron diseñados para hacernos la vida más fácil, aunque estemos descubriendo rápidamente que en realidad nos están generando problemas que no habíamos imaginado. La pretendida inocencia de estas aplicaciones como la, tantas veces considerada, neutralidad de los datos y de la tecnología no es tal.

Es a partir de aquí donde este mundo apasionante y vibrante se enreda en un laberinto que denominamos *ética*. ¿Para qué nos es útil la ética? Esencialmente para tomar decisiones. 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?

En la era de *big data*, sin embargo, muchas de las decisiones que afectan a nuestro día a día no son tomadas por nosotros mismos, sino por modelos matemáticos que están siendo no sólo programados sino entrenados para tomar decisiones de forma independiente. El problema, en este caso como en muchos otros en los que los algoritmos ocupan la posición del “sujeto moral”, es que cuando nos dispongamos a identificar a un “sujeto responsable” de la acción ejecutada nos veremos ante una máquina. Y sin responsabilidad que atender, la pregunta fundamental de la ética habrá quedado reducida a un mero automatismo.

Esta evidencia ¿destierra definitivamente la ética como disciplina académica? O bien, por el contrario, ¿hará que emerja de sus cenizas para hacerse cargo de una realidad que acontece y muta cada día más y más rápido? Hay al menos tres problemas fundamentales que deben ser confrontados con cierta urgencia por la **ética aplicada a la gestión de datos**: en primer lugar, pensamos en la propiedad de los datos. ¿A quién pertenecen los datos, a quienes los generan, a quienes los almacenan o a quienes los compran? ¿Quién está autorizado a vender datos? Este asunto se está transformando en un asunto técnico legal en tanto que ya existen sentencias que se posicionan claramente del lado de los usuarios y no tanto de las redes sociales o las empresas. En cualquier caso, la ética sigue siendo necesaria en este caso para anticiparse a algo que no podrá nunca estar regulado en su totalidad, precisamente por aquello que caracteriza a los *big data*: su volumen y velocidad.

El segundo problema atiende a la privacidad; muy relacionado con la propiedad, la privacidad y protección de datos sensibles ha pasado a depender en muchos casos de las empresas, que han desplazado al Estado en su cometido

de velar por nuestra seguridad. El contrato social se ha transformado en un contrato real de suministro de servicios. De nuevo, será un problema esencialmente técnico legal.

Hay un tercer problema, a nuestro parecer el más grave de todos y en el que descansa la confrontación eficiente de los anteriores y que no es otro que la dificultad para identificar al sujeto moral, es decir, del sujeto que debe asumir responsabilidad, hacerse cargo de la realidad y de las consecuencias que se generan con su acción, ya ocurra esta durante la generación, la gestión o la utilización posterior del conocimiento generado en el tratamiento de los datos. La figura mitológica del Minotauro, transformado ahora en algoritmos de entrenamiento que están enseñando a las máquinas a aprender, pacientemente, lo mejor y lo peor de los humanos, necesita encontrar una ética preparada para el siglo XXI, y unos profesionales de los datos capaces de ponerla en práctica de forma cotidiana: un Teseo renovado y, ciertamente, transformado.

## Objetivos

Esta asignatura denominada *Ética y big data* tiene como objetivos:

1. Realizar una aproximación a los problemas que debe confrontar una ética de los datos, presentando en primer lugar qué entendemos por ética y cómo podríamos caracterizar al sujeto moral que emerge en este nuevo escenario.
2. Presentar las principales teorías éticas que son inherentes a los principios profesionales. Principios que han de orientar la acción del profesional de los datos: beneficencia, autonomía, no maleficencia y justicia.
3. Analizar los problemas fundamentales que debe confrontar una ética aplicada a los datos: identidad, privacidad, propiedad y reputación.
4. Establecer unos puntos de decisión ética que nos permitan alinear los valores con las decisiones tomadas, y con ello, con las acciones.

Cada uno de estos objetivos es abordado en uno de los cuatro apartados que completan el curso.



# 1. Ética y big data

## 1.1. Introducción

Desde que Boyd y Crawford planteasen en 2012 su «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 adaptada a los cambios que provocarían los avances tecnológicos sobre la calidad y las formas de vida. 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<sup>1</sup>. Los *big data*, como parte de la denominada *Internet of Things*<sup>2</sup> (IoT), deben ser considerados un fenómeno sociotecnológico en tanto que no solo están transformando la cultura de comunicación entre seres humanos, sino que interviene en los espacios privado y público de los agentes haciendo que la frontera entre ambos se muestre más difusa que nunca antes.

### Ética

La ética, tanto personal como organizacional, consiste en la adquisición de conocimientos que van conformando nuestro «carácter», o «cultura» en el caso de las organizaciones, que nos permiten tomar decisiones orientadas hacia el bien, no solo en un momento determinado sino en el conjunto de la vida.

<sup>(1)</sup> Siguiendo a Castells (2009), entendemos 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». M. Castells (2009). *Comunicación y poder* (pág. 38). Madrid: Alianza.

<sup>(2)</sup> Consideramos aquí que lo que se denomina *Internet of Things* (IoT) consiste básicamente en: 1) una tecnología sensible inserta en entidades físicas, objetos cotidianos de uso generalizado, que recopila datos de forma constante; 2) redes que permitan el intercambio de los datos generados por esta tecnología; 3) potencia computacional para la interpretación de esta ingente cantidad de datos (*big data*), y, finalmente, 4) 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 manual se consideran de este modo indistinto la «ética y *big data*» y la «ética aplicada a la IoT». Vid. Tamara Dull, «Big data and the Internet of Things: Two sides of the same coin?». *SAS best practices*: [http://www.sas.com/en\\_us/insights/articles/big-data/big-data-and-iot-two-sides-of-the-same-coin.html](http://www.sas.com/en_us/insights/articles/big-data/big-data-and-iot-two-sides-of-the-same-coin.html) [Fecha de consulta: 21 de diciembre de 2015].

### Lecturas recomendadas

D. Boyd; K. Crawford (2012). «Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon». *Information, Communication & Society* (vol. 15, núm. 5, págs. 662-679).

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

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

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

Las estructuras sociales que comienzan a manifestarse a partir de la gestión, disponibilidad y uso de los *big data* hacen emerger conflictos éticos en muchos casos heredados de la **ética de los negocios**, aunque ahora esta se vea supera-

da por las circunstancias en las que operan la generación y gestión masiva de datos. *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 la empresa debe desarrollar una cultura ética específica que asista en la toma de decisiones. En la medida en que almacenar, gestionar y utilizar datos (en muchos casos con 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 manera 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 de estas<sup>3</sup>.

<sup>(3)</sup>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 porque se considera «útil» para favorecer la reputación y con ello la confianza de consumidores, clientes y/o proveedores. Este enfoque utilitarista de la ética como «inversión rentable» ha sido desarrollado, entre otros, por Adela Cortina, quien mantiene que las empresas han comprendido que la credibilidad es fundamental para la sostenibilidad de su actividad, y la credibilidad es un valor ético en cuanto que se sustenta en la confianza y la responsabilidad. Esta concepción se aleja de la necesaria incorporación de la ética a la cultura de la empresa, 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.

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 *big data* tienen grandes dificultades para llegar a estar regulados legalmente? Y ello, precisamente, por lo que los caracteriza, esto es, lo que se denominan las 4 V: volumen, variedad, velocidad y valor. ¿Es lo mismo «bueno» que «correcto»?

Como han apuntado Weil y Haarkötter (2014), hay dos problemas fundamentales que deben ser confrontados por una ética aplicada a la denominada IoT:

- 1) determinar en qué realidad se ubica este campo de reflexión ética e
- 2) identificar al sujeto o sujetos a quienes se podrán atribuir tanto la toma de decisiones como la responsabilidad que de ellas puedan derivarse.

Estas son las dos cuestiones que intentaremos tratar en este primer capítulo. Nos ocuparemos primero de delimitar las áreas en las que podemos establecer que opera esta ética aplicada a la IoT, o a los *big data*. Para ello, nos situaremos

#### Lectura recomendada

M. Mortazavi; K. Salah (2015). «Privacy and Big Data». En: S. Zeadally; M. Badra (eds.). *Privacy in a Digital, Networked World. Technologies, Implications and Solutions* (págs. 37-55). Springer.

#### Lectura recomendada

F. Weil; H. Haarkötter (2014). «Ethics for the Internet of Things». *International Review of Information Ethics* (núm. 22, págs. 2-5).

en el marco más amplio que nos facilita lo que Bielby (2014) denomina una «taxonomía» de la ética aplicada a los sistemas de información. 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 buena, por emplear un término aristotélico y comenzar a entrar ya en materia.

Ello nos permitirá comprender el sentido de lo que denominamos «sujeto moral». Aunque es habitual el uso indiferenciado de los términos *ética* y *moral*, es cierto que en muchas ocasiones hemos escuchado a nuestros estudiantes, e incluso a colegas, expresar esta duda respecto a cómo diferenciar entre *ética* y *moral* o si es realmente necesaria esa distinción. El problema no parece residir, sin embargo, en distinguir una de otra, sino más bien en no comprender el sentido de ninguna de las 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 de los big data**.

## 1.2. ¿Dónde ubicar una ética de los big data?

Es posible considerar la filosofía de la IoT, o de los *big data*, como una parte de la filosofía 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 grandes colecciones de datos, o *big data*, que se obtienen en el espacio de la IoT. Así, mientras ontología y epistemología pueden considerarse en un nivel «interno» a esta ciencia de los datos, la ética es «externa» en cuanto que se ocupa de las consecuencias de la actividad a la que dan soporte, siquiera teórico, las dos primeras, tanto en individuos, como en organizaciones, en comunidades o en la sociedad en general.

La **ética aplicada a la IoT** puede considerarse como una ética de ámbito profesional en la medida en que se ocupa esencialmente de la responsabilidad de determinados grupos de expertos, pero también tendría una parte de ética empresarial porque 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**; 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. Pero en ella operan necesariamente, además, problemas y reflexiones propios de la ética de los sistemas de

### Lectura recomendada

J. Bielby (2014). «Towards A Unified Taxonomy» [en línea]. En: *Information Ethics*. University of Alberta. [Fecha de consulta: 28 de marzo de 2016]. [https://www.academia.edu/4896164/Information\\_Ethics\\_II\\_Towards\\_a\\_Unified\\_Taxonomy](https://www.academia.edu/4896164/Information_Ethics_II_Towards_a_Unified_Taxonomy)

### Lectura recomendada

M. Swan (2015). «Philosophy of Big Data». En: *2015 IEEE First International Conference on Big Data Computing Service and Applications* (págs. 468-477). IEE Computer Society.

### Lectura recomendada

S. Zamagni (2008). *Por una economía del bien común*. Madrid: Ciudad Nueva.

D. J. Michelini (2008). *Bien común y ética cívica, una propuesta desde la ética del discurso*. Buenos Aires: Bonum.

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<sup>4</sup>.

<sup>(4)</sup>Ved la documentación disponible en «Publicaciones» de la página web del International Center for Information Ethics: <http://icie.zkm.de/publications/> [Fecha de consulta: 31 de marzo de 2016].

La reflexión ética que corresponde a esta IoT podría mapearse de acuerdo con la siguiente taxonomía:

1) 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 de las redes sociales, la ética de la IoT e incluso la ética aplicada a la robótica. Capurro y otros (2013) han identificado unos valores que operan de manera 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. Estos autores conciben la ciberética como una «teoría sobre la libertad en el medio digital».

2) La «ética de la computación» comparte espacios con la ciberética, en cuanto que se ocupa de la tecnología que se emplea para la recopilación, la gestión y el tratamiento de los datos, pero sin ceñirse a internet, es decir, se ocupa de los problemas éticos que surgen en el desarrollo y la utilización de herramientas computacionales en todos los ámbitos de la sociedad.

3) La ética de la información en investigación biomédica, como parte de la bioética, sería aquella que se ocupa de analizar la interacción entre seres vivos y técnicas digitales.

### 1.3. 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, con quien nos da acceso a la sociedad red. 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 o como clientes y/o proveedores. ¿Quién debe asumir entonces la condición de sujeto moral en la ética de los *big data*? Todo apunta a que será, ineludiblemente, una combinación de todos estos tipos.

#### 1.3.1. 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

#### Lecturas recomendadas

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

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

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, que todas y cada una de las personas tienen razones para valorar como «convenientes» de cara a conformar su 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<sup>5</sup> o de Rousseau, en su obra *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».

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?

Esta idea nos puede ayudar a comprender el sentido del primer término empleado para referirse a «ética». El primer *éthos* (*ἦθος*) 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. 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».

¿Cómo podría sernos útil esta noción espacial al abordar la ética de los *big data*? ¿Cómo si los *big data* se dan en un entorno no físico, que de algún modo nos dificulta revelarnos como «sujetos morales»?

¿Por qué decimos, además, que nuestra condición humana es inherentemente moral? Siguiendo a Aranguren porque 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

<sup>(5)</sup>Ved la ilustración que acompañó a la primera edición de su *Leviatán* (1651): una idea de Estado que como un gigante construye por sí mismo un paisaje compuesto por cientos de pequeños individuos.

#### Lectura recomendada

M. Zambrano (2004). *Persona y democracia* (pág. 122). Madrid: Siruela, 1958.

#### Lectura recomendada

M. Heidegger (2001). *Carta sobre el Humanismo* (págs. 72-83). Madrid: Alianza, 1947.

la dimensión moral que nos es inherente a todos los seres humanos. Nuestra capacidad para decidírnos entre irrealidades posibles, distinguiendo entre el bien, el mal y/o aquello que atiende exclusivamente a nuestros intereses.

¿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 por «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 *êthos*. El *êthos* como carácter, como modo aprendido de vivir, procede del *êthos*, 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. En latín *êthos* 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.

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 su argumento prefilosófico, «el hombre es constitutivamente moral porque es constitutivamente libre, tiene por fuerza que hacerse –suficiente o insuficientemente– su propia vida». La «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 una filosofía práctica denominada Ética.

#### Lectura recomendada

J. L. Aranguren (1994). *Obras Completas*. Vol. II: *Ética* (págs. 172-177). Madrid: Trotta.

#### Lectura recomendada

X. Zubiri (1944). *Naturaleza, Historia, Dios* (pág. 259). Madrid: Ed. Nacional.

Esta Ética, con mayúscula, podría establecerse 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. Como vimos en el primer epígrafe, la **ética de los big data** formaría parte de lo que se ha denominado **teorías éticas en el campo de la información**.

### 1.3.2. ¿Un giro copernicano para la ética de los big data?

La ética que debe desarrollarse para generar comportamientos orientados al bien en este nuevo escenario debe plantearse críticamente tanto los supuestos que se dan por válidos como los sesgos o predisposiciones habituales. El planteamiento revolucionario que planteábamos en la introducción parece exigir un nuevo «giro copernicano» en cuanto que exige una anticipación para la que los humanos no estamos (ya) preparados, no al menos si hemos de competir en la toma de decisiones con algoritmos.

Eso que Bauman (2006) ha denominado «el encubrimiento tecnológico del yo moral» entiende 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 la medida en 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». Esto implica que no sea posible la responsabilidad, ni por ese Otro, ni por el mundo. Esta fragmentación, en cuanto que encubrimiento de la naturaleza sistémica del hábitat humano y con ello del desmembramiento del yo moral, es una de las principales causas, mantiene Bauman, de lo que Beck (1992) denominó «sociedad riesgo»<sup>6</sup>.

<sup>(6)</sup>A diferencia de «peligro», el «riesgo» pertenece al discurso de los «juegos de azar», eludiendo la oposición entre «éxito y fracaso» o entre «seguridad y peligro». Ello potencia la visión del mundo como un juego, y estar en el mundo, como jugar.

#### Lecturas recomendadas

**Z. Bauman** (2006). *Ética pos-moderna* (pág. 225). Madrid: Siglo XXI.

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

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

### 1.4. Conclusiones del apartado 1

Hemos establecido y definido el contexto de una ética de los *big data*, como una ética de la IoT, en el ámbito de una ética de los sistemas de información. Se ha argumentado sobre aquello que distingue ética y moral a partir de un

argumento etimológico. Todo ello nos permite establecer algunos principios desde los que confrontaremos los problemas concretos de la ética de los *big data*:

1) Hemos diferenciado entre una ética del ciberespacio, ciberética, una ética de la computación y la bioética.

2) El «sujeto moral» no puede verse reducido a un mero individuo que opera en los espacios dicotómicos privado/público. Las fronteras no son solo más borrosas entre espacios de responsabilidad, sino que dichos espacios se multiplican y se unifican en cuanto que su porosidad y fragmentación es lo que mejor los caracteriza.

3) Además, hemos sostenido que este «nuevo» sujeto es tan constitutivamente moral y social como su antecesor. Ello implica que consideramos que en la IoT operan seres humanos que toman decisiones, 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. De ello nos ocuparemos en el siguiente apartado, cuando abordemos los principios profesionales que deben operar en una ética aplicada y profesional como la que nos ocupa.



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

### 2.1. 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<sup>7</sup>, o bien ordenada –justa, libre, próspera–, si seguimos a Rawls, 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 manera simultánea, personas buenas, que cumplen en lo moral. La pregunta fundamental de la ética nos confronta entonces como profesionales y como personas. No hay posibilidad alguna de eludir esta condición inherentemente humana si no es incurriendo en el riesgo de desprendernos precisamente de una parte de 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 que adopta Howard Gardner para explicar la necesaria conexión entre los ámbitos público y privado a través del valor de «virtud» 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 que sea excelente en calidad, socialmente responsable y que contribuya a la realización como persona de quien lo lleva a cabo<sup>8</sup>.

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 apartado, interpelar a aquellos que 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 apartado de este módulo.

<sup>(7)</sup>El concepto de sociedad decente se basa 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», aquella en la que las instituciones no humillan a las personas.

#### Lectura recomendada

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

<sup>(8)</sup>Una conceptualización que arranca de la idea de eudaimonía y florecimiento humano. Ved The good Project, <http://www.thegoodproject.org/projects/the-good-work-project/>.

## 2.2. Teorías éticas. Breve introducción

Del mismo modo, en aquel primer apartado, 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 los *big data*. Entre otras, aquella que cuestionaba 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.

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» o «teoría del bien»; 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», y 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 lo que se considera como un «valor».

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», lo que les permite identificar lo correcto con la maximización de dicho bien (o valor), es decir, la elección del agente debe estar 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.

Veamos un ejemplo:

### Las «teorías éticas»

No deben comprenderse como un catálogo de opciones para aproximarnos a la «ética», lo que equivaldría a cierto relativismo moral en cuanto podrían considerarse todas y cada una de ellas con razones suficientes y plausibles a su favor. Las «teorías éticas» tratan, más bien, de explicarnos desde la filosofía moral, es decir, desde la «ética pensada» (*ethica utens*), diferentes conceptualizaciones 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.

### Lectura recomendada

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

### Lectura recomendada

J. F. Bonnefon; A. Shariff; I. Rahwan (2016). «The social dilemma of autonomous vehicles» [artículo en línea]. *Science* (vol. 352, núm. 6293, págs. 1573-1576). <http://science.sciencemag.org/content/352/6293/1573.full> [Fecha de consulta: 21 de noviembre 2016].

**Lectura recomendada**

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

Un dilema moral establece como valor «salvar vidas», planteando dos posibilidades para la acción: una ofrece la probabilidad del 50 % de salvar cien vidas, y otra, la probabilidad de salvar un total de cuarenta vidas con una certeza del 100 %. 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<sup>9</sup>. 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 minimización implica muchas veces sacrificar al propio conductor del vehículo y a 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 «correcta».

<sup>(9)</sup>Ved Moral Machine Project, Massachusetts Institute of Technology (MIT): <http://moralmachine.mit.edu/> [Fecha de consulta: 21 de noviembre de 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 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 cuanto 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.

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.

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.

### 2.3. Principios orientadores de la acción del buen profesional

Las teorías éticas a las que hemos aludido 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 concretos que afectan a vuestra profesión como analistas de *big data*, abordaremos cuatro principios profesionales que emanan de la bioética, la ética profesional con mayor trayectoria y desarrollo. 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.

¿Por qué apelar a unos principios en una época en la que los datos, y más aún los *big data*, 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.

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, tenemos el **principio de beneficencia**. Este principio puede entenderse en términos consecuencialistas, o utilitaristas, donde el «bien» es identificado 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

#### Lecturas recomendadas

A. Jonsen (1998). *The Birth of Bioethics*. Nueva York: Oxford University Press.

A. Hortal (2002). *Ética de las profesiones* (pág. 95). Bilbao: Declée de Brower.

**principio de no maleficencia** puede resultarnos especialmente útil en caso de no ser posible la aplicación de los anteriores, aplicando la máxima «ante todo no hacer daño».

¿Cómo deben aplicarse estos principios? Siguiendo a Hortal (2002), podríamos decir que 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». 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.

### 2.3.1. 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<sup>10</sup>. Por ello es importante saber identificar aquellos valores y/o bienes que consideramos que **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.

<sup>(10)</sup> La *Ética a Nicómaco* comienza con toda una declaración de principios sobre aquello que «mueve» la acción humana: «Parece que toda 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».

De manera simultánea deberán considerarse las consecuencias de dicha acción, es decir, los beneficios y los daños que puedan generarse, aun con una finalidad orientada al bien, 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<sup>11</sup>».

#### Lectura recomendada

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

#### Valores o bienes que deben ser promovidos

Encontramos aquí una nueva cuestión ética: ¿Qué bienes pretendemos alcanzar con nuestro trabajo?

#### Lectura recomendada

Aristóteles (2014). *Ética a Nicómaco* (Libro I, 1094a, pág. 57). Edición de J. L. Calvo Martínez. Madrid: Alianza Editorial.

#### 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 asumidos por el resto de las éticas aplicadas a las diferentes actividades profesionales.

<sup>(11)</sup>*The Belmont Report: Ethical Guidelines for the Protection of Human Subjects of Research* [en línea]. Washington D. C.: Department of Health, Education, and Welfare. <http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/> [Fecha de consulta: 24 de noviembre de 2016]. Existen diferentes versiones accesibles en castellano, entre otras la del Observatori de Bioètica i Dret de la Universitat de Barcelona: <http://www.bioeticayderecho.ub.edu/archivos/norm/InformeBelmont.pdf> [Fecha de consulta: 24 de noviembre de 2016].

Si recordamos la definición de ética, vista en el primer apartado, 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 quien se dirige nuestra actividad).

### 2.3.2. 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 autonomía como el valor que guiará el cambio de época que emerge tras las revoluciones americana y francesa. ¡Atrévete a pensar por ti mismo!, exhorta Kant en su pequeño ensayo «Respuesta a la pregunta: ¿Qué es la Ilustración?» (1784), estableciendo con ello los cimientos de la estrecha urdimbre que conforman libertad y responsabilidad para la idea de ciudadanía que viene. 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 arts. 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:

#### Lectura recomendada

I. Kant (2007). «Respuesta a la pregunta: ¿Qué es la Ilustración?». En: I. Kant. *¿Qué es la Ilustración? Y otros escritos de ética, política y filosofía de la historia* (págs. 83-93). Edición, traducción y estudio preliminar de Roberto R. Aramayo. Madrid: Alianza Editorial, 1784.

«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».

**Lectura recomendada**

V. Camps (2005). *La voluntad de vivir* (págs. 110-114). Barcelona: Ariel.

La autonomía que debemos considerar aquí, en cuanto 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:

- 1) el sujeto debe tener capacidad racional para elegir críticamente entre diferentes cursos de acción;
- 2) debe poseer habilidades, mentales y/o físicas, para alcanzar los fines «elegidos»; y, finalmente,
- 3) 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*).

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 afectan a su cliente/paciente sin atender sus propios criterios e, incluso, sin su consentimiento.

En nuestro campo 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, etc.

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. 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.

### 2.3.3. 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 como y 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** hasta la actual bioética.

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 será 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– cuando pueda hablarse de una ética racional auténticamente deontológica. Una ética 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.

#### Lectura recomendada

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

#### El Corpus hipocrático

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. No obstante, los expertos coinciden en atribuir a este autor únicamente cuatro de estas obras: *Epidemias I y III*, *Pronóstico* y *Sobre la dieta en las enfermedades agudas*. Ved C. García Gual (ed.) (1983). *Tratados Hipocráticos*. Madrid: Gredos.

#### Lectura recomendada

D. Gracia (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 [en línea]. Madrid: Anzos. <http://bibliotecavirtual.ranm.es/ranm/es/consulta/registro.cmd?id=617> [Fecha de consulta: 30 de noviembre de 2016].



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. 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-constraints* 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.

#### Lectura recomendada

R. Nozick (1988). *Anarquía, Estado y utopía*. Ciudad de México: Fondo de Cultura Económica, 1974.

Lo que viene a mostrar Gracia es que 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. Por el contrario, el principio de no maleficencia es esencialmente deontológico en la medida en que alude a principios universales que han de comprenderse como anteriores 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**.

#### Vacunar o no vacunar

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, de 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 6 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. Ved «El Comité de Bioética recomienda ampliar la obligación de vacunar» [en línea]. *El País* (9 de febrero de 2016). [http://politica.elpais.com/politica/2016/02/09/actualidad/1455036981\\_427745.html](http://politica.elpais.com/politica/2016/02/09/actualidad/1455036981_427745.html) [Fecha de consulta: 29 de noviembre de 2016].

### 2.3.4. 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 cuanto que existe un mandato que está por encima de nuestra libertad y autonomía que nos lo impide.

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. La justicia, y aquí volvemos a (Gracia, 1990, pág. 74), 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».

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.

La norma universal, deontológica, que opera en los principios que funcionan con absolutos nos permite distinguir entre lo «correcto» y lo «incorrecto»; mientras que la aplicación de dicha norma a un caso concreto puede llevarnos a decidir si aplicar una excepcionalidad a la norma y, aplicando la teoría consecuencialista, llegar a un resultado «bueno», para el caso, en vez de algo que de aplicar la norma sería necesariamente «malo».

### 2.4. Conclusiones del apartado 2

En este apartado se han abordado primero las dos principales teorías éticas que tradicionalmente se han disputado la hegemonía en la toma de decisiones: consecuencialismo y deontología. Hemos visto por qué ambas podrían tener problemas si se siguiesen de forma escrupulosa. También hemos presentado una teoría alternativa que trata de mediar entre ambas formas de comprender la ética aplicada a la toma de decisiones: la ética dialógica y las soluciones que propone.

#### Lectura recomendada

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

A continuación se han presentado los cuatro principios orientadores de la acción profesional, que tomamos de la bioética, la ética profesional con mayor trayectoria en diagnosticar y confrontar problemas para una correcta alineación de valores y acción. Los principios pueden ser agrupados en dos parejas:

1) Beneficencia y autonomía.

2) No maleficencia y justicia.

Si en la primera pareja prevalece la teoría consecuencialista limitada por la autonomía, en la segunda prevalece el principio deontológico limitado por la idea de justicia.

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, tenemos el **principio de beneficencia**. Este principio puede entenderse en términos consecuencialistas, o utilitaristas, donde el «bien» es identificado y la finalidad de la acción del profesional es, ante todo, lograr su maximización. Habitualmente entra en conflicto con el denominado **principio de autonomía**, 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. Muchas veces, sin embargo, la mera consideración de la autonomía no es suficiente, bien porque se generan situaciones injustas, bien porque una decisión individual pueda poner en riesgo a toda una comunidad. Es entonces cuando es preciso 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 al **principio de no maleficencia**, de clara inspiración deontológica, y que puede resultarnos especialmente útil en caso de no ser posible la aplicación de los anteriores, aplicando la máxima «ante todo no hacer daño». Este último principio es actualmente considerado el más apropiado para orientar la toma de decisiones éticas en los ámbitos profesionales.

Se han presentado ejemplos y casos relacionados con los *big data* pero también debe comprenderse como un apartado que nos dota de herramientas para comprender cómo aplicar o hacer efectivos los problemas derivados del uso de *big data*, que veremos en el apartado siguiente.

### 3. Conceptos fundamentales para una ética aplicada a *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)

«La ley no reemplaza la conciencia». (Edward Snowden)

#### 3.1. 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 los dos primeros apartados de este módulo, esperamos que esta afirmación no os deje indiferentes. Los datos tienen una fuente, son obtenidos 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 accesibilidad<sup>12</sup>. Actualmente, estos problemas, con la eclosión de la IoT, podrían ser reformulados en identidad, privacidad, propiedad y reputación. Davis (2012) considera que estos cuatro problemas pueden ser considerados la estructura esencial de una ética aplicada a los *big data*. El tamaño y la omnipresencia de estas **grandes colecciones de datos** 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.

#### 3.2. Identidad

La proposición ética precisa un sujeto moral que se haga cargo de la realidad mediante una respuesta responsable. Ese sujeto moral, humano, debe asumir la doble máxima del oráculo de Delfos: «Nada sin medida» y «Conócete a ti

<sup>(12)</sup>Mason utilizaba el acrónimo PAPA para referirse a estos cuatro aspectos éticos: *privacy*, *accuracy*, *property* y *accessibility*.

#### Big data

Entendemos *big data* como una constelación de fenómenos relacionados con la producción, el consumo, la recopilación y el 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.

#### Lecturas recomendadas

R. O. Mason (1986). «Four Ethical Issues of the Information Age». *Management Information Systems Quarterly* (vol. 10, núm. 1, págs. 5-12).  
K. Davis (2012). *Ethics of Big Data*. Sebastopol, CA: O'Reilly Books.

mismo»; ancestrales comentarios de la proposición ética que nos exige «armonizar la conducta con la naturaleza y carácter de la *humana conditio*», esto es, aquella que nos permite asumir nuestra humanidad.

Trías (2000) explica 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; finalmente, el sujeto III, argumenta, o justifica que 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 *big data*. 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: **prosumers**. ¿Qué 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?

### 3.2.1. Una dirección IP no da cuenta de nuestra identidad

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. 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 de 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?

#### Lectura recomendada

E. Trías (2000). *Ética y condición humana* (pág. 82). Barcelona: Ediciones Península.

#### Prosumers

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 *big data* son, además, los productores de los datos que conforman los repositorios de *big data*.

### 3.2.2. La identidad se moldea en el tiempo y en el espacio-red

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 consideran los gestores de esas redes sociales. 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 todos los datos generados en el curso de la vida de una persona interactuando con un dispositivo, aquello que algunos denominan el Yo cuantificado<sup>13</sup>. La identidad que surge entonces ¿es necesariamente prismática o, por el contrario, solo si es única podremos considerarnos personas íntegras?

<sup>(13)</sup>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». 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 3.000 fotografías al día. Citado por E. Morozov (2015). «La condición superhumana». En: *La locura del solucionismo tecnológico* (págs. 209-349). Madrid: Katz Editores. ¿Podemos considerar esto que Bell denominó *Lifeloggging* 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? Respecto a esta cuestión, ved G. Bell; J. Gemmell (2010). *Your Life, Uploaded: The Digital Way to Better Memory, Health, and Productivity*. Nueva York: Penguin Books.

#### Perdurabilidad en el tiempo

La Biblioteca del Congreso de 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.

Estas dos visiones diametralmente opuestas son las que mantienen, respectivamente, Christopher Poole y Mark Zuckerberg<sup>14</sup>. Aunque resulte paradójico, ambas interpretaciones comprenden las transformaciones que el fenómeno *big data* está aportando al concepto de identidad: en la medida en que *big data* 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 de 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 que 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.

<sup>(14)</sup>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 en torno al concepto de «identidad poliédrica», ved Tim Carmody, «You are not your name and photo, a call to re-imagine identity» [en línea]. WIRED (20 de noviembre de 2010). <https://www.wired.com/2011/10/you-are-not-your-name-and-photo-a-call-to-re-imagine-identity/> [Fecha de consulta: 8 de diciembre de 2016]. 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. Vease M. Helft (2011, 13 de mayo). «Facebook, foe of anonymity, is forced to explain a secret» [en línea]. *The New York Times*. <http://www.nytimes.com/2011/05/14/technology/14facebook.html> [Fecha de consulta: 8 de diciembre de 2016].

Nos hemos referido aquí hasta ahora al riesgo en el que incurren los individuos, sin embargo, usuarios *consumers* 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 de los datos recogidos, de sus pacientes, estudiantes, ciudadanos o clientes, como de los datos ya gestionados con una intención concreta. La identidad de estos *consumers* 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?

### 3.3. Privacidad

Los seres humanos valoramos nuestra privacidad y la protección de la esfera más íntima de nuestra propia vida y de las personas que consideramos más próximas. Pretendemos mantener cierto control sobre quién sabe qué sobre nosotros mismos. Sin duda, no deseamos que nuestra información personal sea accesible a cualquier persona en cualquier momento. Del mismo modo que entendemos que tanto *big data* como la tecnología en general están modificando el sentido y el significado de lo que llamamos «identidad», hemos de considerar la influencia sobre el concepto que engloba el término *privacidad*.

Gracias a los medios de comunicación digital es posible argumentar que el grado de control sobre cómo percibimos la realidad se ha incrementado; esto mismo nos permite, a su vez, ser percibidos con mayor transparencia y precisión: la imagen de Snowden, por ejemplo, no es construida a partir de una sola fuente sino que disponemos de una pluralidad suficiente como para no considerar únicamente la imagen que de él ofrece el gobierno de Estados Unidos<sup>15</sup>. Sin duda, esto es positivo y amplía las oportunidades para la construcción de una visión crítica de la realidad. Sin embargo, ¿representa esto un mayor o un menor control sobre cómo se nos percibe, cómo se construye nuestra propia identidad al fin y al cabo, en la red?

#### Consumers

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*. *Consumers* son 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 manera simultánea es un consumidor de datos producidos por los mismos usuarios (*prosumers*) a los que da servicio.

<sup>(15)</sup>Edward Snowden, técnico informático que trabajó para la CIA y la NSA, agencias de información del Gobierno de Estados Unidos, reveló a los periódicos *The Guardian* y *The Washington Post*, en junio de 2013, los programas de vigilancia masiva que estaban siendo utilizados ilegalmente por estas agencias. Ved «The Snowden Files» [en línea]. *The Guardian*. Recopilación de documentos relacionados con las revelaciones de Snowden. <https://www.theguardian.com/world/series/the-snowden-files> [Fecha de consulta: 9 de diciembre de 2016].

Efectivamente, en la red ya no somos lo que nosotros pretendemos ser; nuestra identidad, como vimos en el anterior epígrafe, 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. ¿Quién tiene acceso a nuestros datos?, ¿con qué finalidad se facilita ese acceso?, ¿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?

La famosa viñeta que Steiner publicó en *The New Yorker* en 1993 y en la que un perro frente a un PC le dice a otro, que lo 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<sup>16</sup>. Actualmente, *big data* no solo nos permitiría conocer que se trata de un perro, sino su raza, sus galletas favoritas, si ha ganado algún premio en algún concurso canino, sino que incluso se aventurará a «adivinar», a través de algoritmos, cuáles son las noticias que lo harán reaccionar positivamente en Facebook, qué libros leerá o qué ropa comprará.

<sup>(16)</sup>Ved Michael Cavanaugh: «NOBODY KNOWS YOU'RE A DOG: As iconic Internet cartoon turns 20, creator Peter Steiner knows the idea is as relevant as ever» [en línea]. *Washington Post* (31 de julio de 2013). <http://wpo.st/N8vJ2> [Fecha de consulta: 7 de diciembre de 2016].

### 3.3.1. Privacidad *offline* frente a *online*

¿Tiene el término *privacidad* un significado unívoco *online* y en el mundo real, esto es, *offline*? Podemos abordar esta discusión comparando el comportamiento habitual de las personas respecto a su intimidad cuando están *offline*, con las expectativas que mantenemos cuando estamos *online*. Del mismo modo que exigimos a otros una justificación razonable por haber transformado información privada en información pública, podríamos preguntarnos: ¿por qué no aplicamos del mismo modo nuestra capacidad para autoseleccionar y controlar qué facetas de nuestra intimidad compartimos en el mundo real, *offline*, cuando estamos *online*? ¿Qué valor puede tener para las personas perder el control sobre sus datos, dejando que otros los utilicen de un modo supuestamente innovador y beneficioso para la mayoría, si con ello incurren en riesgo de que esos mismos datos sean utilizados para hacerles daño?



Podríamos considerar una proposición ética aquella que nos lleva a considerar que nuestras expectativas *offline* respecto a la identidad y la privacidad deben reflejarse en nuestra capacidad para gestionar nuestro comportamiento *online*, manteniendo al menos funcionalmente aquellas expectativas. La cuestión es ¿es posible atender esta proposición? La distancia significativa que se da entre las expectativas que mantenemos respecto a nuestra intimidad *online* y aquellas que hacemos efectivas *offline* es, de hecho, un problema profundamente ético. Lo es porque nuestras expectativas tratan sobre aquello que «debería ser», lo que anhelamos que sea, para poder replicar el estricto control que ejercemos sobre nuestra intimidad en el mundo real-no virtual. Ética también porque tiene que ver con los hábitos y las costumbres en las que nos hemos educado como usuarios. De hecho, aún a muchos, no expertos, les resultará creíble la viñeta de Steiner. En los años noventa fue posible porque la tecnología nos permitía operar en un anonimato casi completo en internet, ahora *stricto sensu* contrario, la red nos hace sentirnos más vulnerables que nunca respecto a nuestra intimidad. El objetivo es entender cómo equilibrar los beneficios de las innovaciones que representa *big data* con los riesgos inherentes para nuestra intimidad que supone compartir más información, más variada y más rápido. Para lograrlo, será preciso explorar aquello que consideramos valioso de aquello que denominamos intimidad en *offline*, para poderlo transformar en condiciones de privacidad *online*.

### 3.3.2. Problemas de privacidad generados por *big data*

Los recientes avances en la tecnología de la información amenazan la privacidad y han reducido el control sobre los datos personales, incrementando el riesgo de efectos negativos sobre la privacidad. El siglo XXI es el siglo de *big data*, y la tecnología de la información avanzada permite el almacenamiento y procesamiento de exabytes de datos. Las revelaciones de Edward Snowden demostraron que estas preocupaciones son reales y que las capacidades técnicas para recolectar, almacenar y buscar grandes cantidades 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 está 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*:

1) Los usuarios no han llegado a comprender cómo afectan las violaciones de privacidad tanto a individuos como al comportamiento social de estos, en gran parte por los problemas que avanzamos en el epígrafe que da entrada a este.

#### Lectura recomendada

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

2) 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 *big data*.

3) Los datos falsos o los resultados de análisis falsos pueden ser compartidos (a menudo de manera automática) en los centros de datos, lo que dificulta que los usuarios puedan ejercer su derecho a corregir o enmendar los errores o falsedades que los afecten mediante un adecuado procedimiento. Por su naturaleza, estas tecnologías hacen posible el monitoreo de todo el mundo todo el tiempo. Como consecuencia, al otorgar al gobierno acceso no restringido a estas tecnologías, 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 tienen una tendencia a violar las expectativas razonables de privacidad si no hay barreras para la intrusión. *Big data* hace que estos problemas cambien de escala, alcanzando unas dimensiones nunca vistas anteriormente.

4) Es posible programar análisis de *big data* 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.

5) Hay un desajuste de las políticas reclamadas por los proveedores, que aquí hemos denominado *consumers*, y los controles reales disponibles para preservar la privacidad de los usuarios.

6) 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.

#### Lectura recomendada

A. J. Feldman; A. Blankstein; M. J. Freedman; E. W. Felten (2012). «Privacy and integrity are possible in the untrusted cloud». *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering* (vol. 35, núm. 4, págs. 73-82).

7) Del mismo modo, existe un incentivo policial similar para utilizar técnicas avanzadas de vigilancia para recopilar datos de manera 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<sup>17</sup>.

#### Lectura recomendada

D. J. Solove (2011). *Nothing to hide* (págs. 32-34). New Haven: Yale University Press.

#### Lectura recomendada

K. Crawford; J. Schultz (2013). «Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms». *Boston College Law Review* (vol. 55, núm. 1, págs. 93-128).

#### Lectura recomendada

D. Gray; D. Citron (2013). «The right to quantitative privacy». *Minnesota Law Review* (98, págs. 62-144).

#### Lectura recomendada

M. Kosinski; D. Stillwell; T. Graepel (2013). «Private traits and attributes are predictable from digital records of human behavior». *Proceedings of the National Academy of Sciences* (PNAS) (vol. 110, núm. 15, págs. 5802-5805).

#### Lectura recomendada

P. Anthonysamy; P. Greenwood; A. Raschid (2013). «Social networking privacy: understanding the disconnect from policy to controls». *IEEE Computer* (vol. 46, núm. 6, págs. 60-67).

<sup>(17)</sup>Ved R. Capurro; M. Eldred; D. Nagel (2013). *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld*.

8) 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.

9) 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 Estados Unidos**, en la prevención de violaciones del derecho y el interés de las personas a la privacidad.

#### Lectura recomendada

S. D. Warren; L. D. Brandeis (1890). «The Right to Privacy» [artículo en línea]. *Harvard Law Review* (vol. 4, núm. 5, págs. 193-220). [http://www.jstor.org/stable/1321160?seq=1#page\\_scan\\_tab\\_contents](http://www.jstor.org/stable/1321160?seq=1#page_scan_tab_contents) [Fecha de consulta: 9 de diciembre de 2016]. Ved *loc. cit. supra* nota 12.

### 3.3.3. 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 a partir de la década de 1890, justificándose en gran parte aludiendo a razones morales. En las discusiones en las que se ha abordado la privacidad en la época contemporánea, algunos tratan la privacidad 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 cuanto 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 corsetaje tras el que ocultar la dominación, la degradación o el daño físico. Esto

#### Lectura recomendada

K. Chaudhuri; D. Hsu (2010). «Sample complexity bounds for differentially private learning». En: *24th Annual Conference of Learning Theory* (págs. 1-32). JMLR: Workshop and Conference Proceedings.

#### 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».

último ha sido especialmente argumentado por el pensamiento feminista y decolonialista, pero también por quienes denuncian los abusos que se dan en la red amparados por el anonimato de los agresores.

### Lecturas recomendadas

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

A. Allen (1999). «Coercing Privacy». *William and Mary Law Review* (vol. 40, págs. 723-757).

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

Así, siguiendo a Van den Hoven, podemos establecer las siguientes razones morales para la protección de datos personales y para proporcionar el control directo o indirecto sobre el acceso a esos datos por otros:

**1) 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.

**2) 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 al intercambio de datos personales, así como para 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.

**3) 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.

**4) 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 y otros 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. El sesgo ideológico al que aludían estos autores ha devenido realidad durante la campaña presidencial de 2016 en Estados Unidos. Las noticias falsas, apoyando al candidato republicano o 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,

### Lectura recomendada

J. Van Den Hoven (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.

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, y desechan aquellas que podrían generar conflicto. Muchos analistas han denunciado que este modo de gestionar las noticias, permitiendo que tanto las «verdaderas» como las «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 «post-verdad», 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*.

### Lecturas recomendadas

D. Lazer (2015). «The rise of the social algorithm. Does content curation by Facebook introduce ideological bias?». *Science* (vol. 348, núm. 6239, págs. 1090-1091).

E. Bakshy; S. Messing; L. A. Adamic (2015). «Exposure to ideologically diverse news and opinion on Facebook». *Science* (vol. 348, núm. 6239, págs. 1130-1132).

N. Heller (2016, 18 de noviembre). «The failure of Facebook democracy» [en línea]. *The New Yorker*. <http://www.newyorker.com/culture/cultural-comment/the-failure-of-facebook-democracy> [Fecha de consulta: 29 de noviembre de 2016].

Una gestión irresponsable de la privacidad provoca que los riesgos de daño, desigualdad, discriminación y pérdida de autonomía emerjan fácilmente. Algo que no solo afecta necesariamente 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 *consumers*, 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 traducción a los efectos sociales y su aplicación a las consecuencias inducidas por las acciones intencionales de los agentes.

Por otro lado, casi todos los países disponen de leyes de protección de datos en vigor<sup>18</sup>. 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 ciudadanía digital o un gestor de dispositivos como Apple o Android, lo que hemos denominado *consumer*, será el responsable último ante las autoridades<sup>19</sup>. 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

### Lectura recomendada

W. Pieters; A. Cleeff (2009). «The precautionary principle in a world of digital dependencies». *Computer* (vol. 42, núm. 6, págs. 50-56).

<sup>(18)</sup>Ved 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](http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php) [Fecha de consulta: 9 de diciembre de 2016].

<sup>(19)</sup>Ved *The Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [en línea]. <http://www.oecd.org/internet/ieconomy/oecdguidelinesonthe-protectionofprivacyandtransborder-flows-of-personal-data.htm> [Fecha de consulta: 9 de diciembre de 2016].

privacidad en el software, la arquitectura, la infraestructura y los procesos de trabajo de tal manera que sea mínimamente probable que ocurran violaciones a la privacidad, al menos de modo sistemático<sup>20</sup>.

<sup>(20)</sup>Existen organizaciones no gubernamentales cuyo objetivo es, precisamente, desarrollar soluciones tecnológicas a los problemas de privacidad generados por esa misma tecnología. Ved, por ejemplo, el Electronic Privacy Information Center, con sede en Washington D. C. 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/> [Fecha de consulta: 9 de diciembre de 2016].

Solove (2006) ha propuesto una taxonomía de la vulnerabilidad de la privacidad, de acuerdo con los diferentes momentos de los procesos de información:

- 1) **Recolección** se refiere a la vigilancia e interrogación con objeto de captar datos.
- 2) **Proceso** se refiere a la recopilación, identificación, inseguridad, uso secundario y exclusión.
- 3) **Difusión** afecta a violaciones de confidencialidad, revelación y exposición indebida, facilidad de acceso, chantaje, apropiación y distorsión.
- 4) **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.

Finalmente, 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 que en Europa se conceptualiza la privacidad en términos de «protección de datos», en Estados Unidos se hace 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 problema, sino que invita a proponer diferentes respuestas a la cuestión que plantea por qué los datos deben ser protegidos<sup>21</sup>.

#### Lectura recomendada

D. J. Solove (2006). «A taxonomy of privacy». *University of Pennsylvania Law Review* (vol. 154, núm. 3, págs. 477-560).

<sup>(21)</sup>El marco jurídico fundamental para la regulación de los servicios *online* en la Unión Europea, incluyendo el comercio electrónico, lo encontramos en la Directiva 2000/31/EC: [http://ec.europa.eu/internal\\_market/e-commerce/index\\_en.htm](http://ec.europa.eu/internal_market/e-commerce/index_en.htm) y en la Estrategia Europea para una Comunicación Segura (2006): [http://ec.europa.eu/information\\_society/newsroom/cf/itemlongdetail.cfm?item\\_id=2766](http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766). De estos dos modos de comprender la privacidad da cuenta el 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 este editorial, publicada en ese mismo medio el día 13 de octubre de 2015, «Digital Privacy, in the U.S. and Europe». Ambos textos pueden consultarse en línea: [http://www.nytimes.com/2015/10/09/opinion/european-ruling-is-merely-a-symbolic-victory-for-privacy.html?\\_r=0](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](http://www.nytimes.com/2015/10/13/opinion/digital-privacy-in-the-us-and-europe.html?_r=0) [Fecha de consulta: 10 de diciembre de 2016].

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 complejización. Es evidente que la privacidad es quizá el problema más acuciante en lo que respecta a *big data* y derechos civiles, y esto garantiza que se aprueben nuevos sistemas de leyes o 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<sup>22</sup>.

<sup>(22)</sup>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» [en línea]. Executive Office of the President (mayo de 2016). [https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016\\_0504\\_data\\_discrimination.pdf](https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf) [Fecha de consulta: 11 de diciembre de 2016].

### 3.4. Propiedad y pertenencia

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 los derechos de quienes generan los datos? ¿A quién pertenecen los datos?, ¿a quienes los generan o a quienes pusieron el medio para hacerlos posibles? ¿Pueden los derechos de propiedad de los datos ser transferidos? ¿Y los 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 como derecho o como 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, colectivo 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 *big data*.

### 3.5. Reputación

Hace apenas veinte años la reputación consistía principalmente en aquello que la gente, en general quienes interactuaban con nosotros habitualmente, conocían y pensaban de cada uno de nosotros. A menos que fuésemos famosos por alguna razón, la gran mayoría manejábamos nuestra reputación actuando bien (o mal) en relación con los que nos rodeaban directamente. En algunos casos, una percepción de segundo grado –es decir, cuando terceras personas llegaban a saber aquello que cada uno de nosotros había dicho de nosotros mismos a las personas que conocíamos– tenía alguna capacidad de influencia, en todo caso limitada, en nuestra reputación. De hecho, así sigue siendo en una, cada vez más pequeña, parte de nuestra vida.

Con lo que *big data* contribuye a una radical reconceptualización de aquello que denominamos con el término *reputación*, ya sea personal o empresarial, es el número de personas que pueden formar una opinión sobre qué tipo de persona, o de empresa, somos. Esto implica que nuestra capacidad para administrar nuestra reputación *online* se haya visto reducida proporcionalmente al incremento del alcance que obtienen cada una de nuestras interacciones en la red. De hecho, actualmente hay empresas cuyo modelo de negocio se centra en la «gestión de la reputación<sup>23</sup>». Su idea sobre qué es la reputación está muy cerca del concepto original, obviando la escala que aporta *big data*: se trata de disminuir la brecha entre lo que realmente eres y cómo te perciben las personas. A pesar de que la máxima tiende a minimizar lo complejo de la empresa, la relación entre reputación e identidad, y con ello de privacidad, con todos los problemas a ella ligada que hemos visto antes, no puede ser obviada.

<sup>(23)</sup>Ved, por ejemplo, Reputation Institute, una consultora internacional dedicada a la investigación sobre reputación corporativa: <https://www.reputationinstitute.com/> [Fecha de consulta: 8 de octubre de 2016].



### 3.6. Conclusiones del apartado 3

En este apartado hemos retomado en primer lugar la justificación de por qué es ineludible abordar una ética de *big data*, revisando además lo que hemos denominado la **dinámica de la acción moral** para considerar ahora quiénes pueden adoptar ese rol de sujeto moral en el sistema en el que intervienen los *big data*.

A partir de los cuatro principios éticos fundamentales de la era de la información, identificados por Mason en 1986, hemos abordado de forma meticulosa los problemas de **identidad, privacidad, propiedad y reputación** que han surgido de la eclosión de la IoT en la vida cotidiana y de la aplicación de tecnologías emergentes en la recopilación, acumulación, producción, consumo y utilización de cantidades masivas de datos, tanto por los denominados *prosumers*, como por los que hemos considerado aquí *consumers*.

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 cuanto 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*.

## 4. La toma de decisiones éticas

### 4.1. Introducción

Las cuestiones que hemos ido planteando a lo largo de este módulo ilustran lo que puede ser una investigación ética. Nuestro método ha tratado de explorar aquello que valoramos de cuestiones problemáticas que surgen de la interacción de las personas con las tecnologías de la información, o lo que aquí estamos considerando *big data*. 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 también 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. La **cultura** de una organización permite hacer explícitos aquellos valores que los miembros de dicha organización sostienen en común. Dichos valores y el desarrollo de una visión común de las acciones que la organización toma para hacer realidad esos valores mediante su actividad influirán 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. Por ello, aquellas organizaciones que asuman con fluidez esta ineludible ética de los *big data* adquirirán el valor estratégico de asumir un papel de líderes en la conducción de la alineación de valores y acciones éticas. ¿Qué procedimientos podrían facilitar esta alineación?

En primer lugar, la transparencia en los procedimientos seguidos por todos aquellos afectados por *big data*, incluidos los usuarios-*prosumers*, repercutirá en el incremento de la confianza y con ella de la reputación de la organización. Del mismo modo, la contabilidad y auditoría de los análisis y de la toma de decisiones que se generan mediante *big data* pueden contribuir significativamente a incrementar la reputación, pero también a minimizar posibles conflictos de intereses o con la justicia. En segundo lugar, podríamos considerar el necesario conocimiento, preciso y actualizado, de la legislación que afecta a *big data*, pero también del origen y de la resolución de los conflictos que generan estos, en la medida en que aún no están sujetos a legislación alguna por su innovación y rápidas transformaciones. Ambas, junto a una estimación abierta de las implicaciones a largo plazo, pueden contribuir significativamente a una reducción en el riesgo de consecuencias no intencionales derivadas del uso de las tecnologías relacionadas con *big data*.

Diseñar innovaciones técnicas, desarrollar nuevas características de producto o tomar decisiones sobre la gestión tiene 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 y operadoras en diferentes áreas solo otorga a Microsoft y Samsung un mero aprobado (5) en transparencia<sup>24</sup>. 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.

<sup>(24)</sup>Ved la interpretación completa de los resultados de la encuesta en «Poniendo nota a las tecnológicas en transparencia e innovación» [en línea], Mónica Tilves, 28 de octubre de 2015: <http://www.silicon.es/poniendo-nota-a-las-tecnologicas-en-innovacion-transparencia-y-algo-mas-infografia-90143> [Fecha de consulta: 12 de diciembre de 2016].

Aunque es totalmente posible que cualquier política dada se alinee con los valores de una organización, no hay manera de saberlo si esta no se hace pública con letra legible. La confusión resultante genera incertidumbre y preocupación, lo que socava las relaciones duraderas y de confianza. Los valores deberían ser asumidos por las organizaciones como el marco de la toma de decisiones, que son necesariamente éticas, simplemente porque los valores representan aquello en lo que las personas creemos, y confiamos. Y creemos en todo tipo de cosas: en la verdad, la justicia, nuestro sistema sanitario, la familia, la amistad. ¿Por qué debería una empresa de *big data* adoptar estos valores en su cultura organizacional?

Antes de que *big data* emergiese con todo su potencial informativo, facilitado a partir del comienzo del siglo XXI con la eclosión y rápida evolución de la IoT, las empresas solían conformarse con cantidades relativamente poco profundas de comportamiento histórico de compra de sus clientes, a menudo limitadas a amplias categorías de información, tales como cuántos de los productos se compraban en un lugar determinado durante un periodo de tiempo específico. Los datos que manejaban las empresas y organizaciones estaban ordenados en filas y columnas, atendiendo a una lógica que los algoritmos han desbaratado totalmente.

*Big data* provee 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 *big data* 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 retuiteamos, entre otras muchas acciones «conectadas». Todo ello facilita una información privilegiada no solo sobre comportamientos y acciones, sino sobre cómo influir mejor

#### B2B, B2C y B2B2C

B2B o *business to business* no se encuentra limitada al entorno electrónico, sino que hace referencia al origen y destino de una actividad, a la relación entre un fabricante y el distribuidor de un producto y también a la relación entre el distribuidor y el comercio minorista.

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 comercio electrónico para comunicar empresas (vendedoras) con particulares (compradores). Por eso, el uso más frecuente es «Comercio electrónico B2C».

B2B2C o *business to business + business to consumer* 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.

en nuestras decisiones futuras, y eso implica una 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 del historial de alquiler a terceros.

En septiembre de 2011, Netflix lanzó 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<sup>25</sup>. 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 de qué modo, en poco más de veinte años, *big data* ha influido en la conformación de nuestros valores y aquello que creemos que es realmente importante para nuestra propia vida. Es precisamente la fuerza de esa conexión entre *big data* y vida cotidiana, y la influencia que esto tiene sobre nuestros valores, lo que debería motivar una discusión más explícita sobre el uso ético de la tecnología asociada a *big data* y del necesario equilibrio entre los beneficios de la innovación y el riesgo de daño.

## 4.2. Puntos de decisión ética

Los puntos de decisión ética proporcionan un marco para explorar la relación entre los valores que entendemos que 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 *big data*. Los puntos de decisión ética se articulan en cuatro actividades que deben entenderse conectadas en bucle, es decir, de un modo no lineal:

- 1) Investigación
- 2) Análisis
- 3) Articulación
- 4) Acción

### Lectura recomendada

N. M. Richards (2015). «Four privacy myths». En: Austin Sarat (ed.). *A world without privacy: What law can and should do?* (págs. 33-82). Cambridge, MA: Cambridge University Press.

(<sup>25</sup>) Citado por K. Davis (2012). *Ethics of Big Data* (pág. 22). Sebastopol, CA: O'Reilly Books. 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>).

La investigación trata sobre la indagación, la discusión y el 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 que 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 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 frecuentemente 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 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 tenemos la intención de utilizar) *big data*, y a 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 cuanto 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:

- 1) **Intención.** Se refiere a las intenciones finales de aquellos quienes por medios directos o subrepticios tienen acceso a los datos.
- 2) **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.
- 3) **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
- 4) **Agregación.** Del mismo modo, la organización debe establecer y hacerse responsable de la combinación de posibilidades derivadas de la correlación de datos disponibles.
- 5) **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.
- 6) **Identidad.** Las colecciones de datos, co- e interrelacionados, que permiten que un sujeto sea caracterizado individualmente.
- 7) **Propiedad.** Trata sobre el estado de la cuestión de quién tiene los derechos de uso en cada punto de la cadena de datos.
- 8) **Beneficio.** Contribución específica positiva de los datos disponibles a la organización, pero también al usuario.

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

El sentido de valores compartidos en una organización, lo que denominamos cultura, reduce las barreras a la productividad y la innovación. En lugar de debatir si debemos hacer algo (es decir, si valoramos colectivamente el objetivo), tenemos derecho a tomar medidas para lograr el objetivo (es decir, trabajar colectivamente para alcanzar la meta).

La Audubon Society y la National Rifle Association tienen objetivos muy diferentes, y sus valores organizacionales son no solo distintos sino controvertidos. Pero hay una característica que ellas, y muchas otras organizaciones, tienen en común: sus respectivos miembros comparten un conjunto de valores. Puede haber desacuerdo entre las filas de vez en cuando, y esos valores pueden cambiar y evolucionar con el tiempo, pero está claro que cada organización dedica una gran cantidad de tiempo a descubrir, articular y tomar medidas basadas en su respectivo conjunto de valores comunes.

Por lo menos una de las muchas razones para este compromiso es que estas organizaciones saben que ser claros y explícitos sobre un conjunto común de valores comunes aumenta su efectividad operativa. Y, del mismo modo, 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 sostiene 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 de la tecnología asociada a *big data* genera cada día.

## 5. Conclusiones finales

Los datos implican a la gente y la gente tenemos valores. Somos seres inherentemente morales, lo hemos repetido casi en cada uno de los apartados que componen este módulo. Por ello, necesitamos disponer de formación y herramientas que nos permitan identificar y confrontar los problemas éticos que emergen de la irrupción de las tecnologías relacionadas con la IoT, los *big data* o *cloud computing*. Con esta asignatura hemos pretendido construir una estructura mínima, aunque esperemos que sólida, que nos facilite establecer y mantener discusiones éticas durante el ejercicio de nuestra profesión como analistas de *big data*. 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

**Aristóteles** (2014). *Ética a Nicómaco*. Edición de José Luis Calvo Martínez. Madrid: Alianza Editorial.

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

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

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

**Bonnefon, J. F.; Shariff, A.; Rahwan, I.** (2016). «The social dilemma of autonomous vehicles». *Science* (vol. 352, núm. 6293, págs. 1573-1576).

**Boyd, D.; Crawford, K.** (2012). «Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon». *Information, Communication & Society* (vol. 15, núm. 5, págs. 662-679).

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

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

**Castells, M.** (2009). *Comunicación y poder* (pág. 38). Madrid: Alianza.

**Davis, K.** (2012). *Ethics of Big Data*. Sebastopol, CA: O'Reilly Books.

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

**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. Madrid: Anzos.

**Heidegger, M.** (2001). *Carta sobre el Humanismo*. Madrid: Alianza, 1947.

**Hortal, A.** (2002). *Ética de las profesiones*. Bilbao: Declée de Brower.

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

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

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

**Kant, I.** (2007). «Contestación a la pregunta: ¿Qué es la Ilustración?». En: I. Kant. *¿Qué es la Ilustración? Y otros escritos de ética, política y filosofía de la historia*. Edición, traducción y estudio preliminar de Roberto R. Aramayo. Madrid: Alianza Editorial, 1784.

**López Aranguren, J. L.** (1994). *Obras Completas*. Vol. II: *Ética* (págs. 172-177). Madrid: Trotta.

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

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

**Michellini, D. J.** (2008). *Bien común y ética cívica, una propuesta desde la ética del discurso*. Buenos Aires: Bonum.

**Mortazavi M.; Salah, K.** (2015). «Privacy and Big Data». En: S. Zeadally; M. Badra (eds.). *Privacy in a Digital, Networked World. Technologies, Implications and Solutions* (págs. 37-55). Springer.

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

**Nozick, R.** (1988). *Anarquía, Estado, y utopía*. Ciudad de México: Fondo de Cultura Económica, 1974.

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

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

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

**Swan, M.** (2015). «Philosophy of Big Data». *2015 IEEE First International Conference on Big Data Computing Service and Applications* (págs. 468-477). IEE Computer Society.

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

**Weil, F.; Haarkötter, H.** (2014). «Ethics for the Internet of Things». *International Review of Information Ethics* (vol. 22, págs. 2-5).

**Zamagni, S.** (2008). *Por una economía del bien común*. Madrid: Ciudad Nueva.

**Zambrano, M.** (2004). *Persona y democracia*. Madrid: Siruela.

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

## Bibliografía en red

**Bielby, J.** (2014). «Towards A Unified Taxonomy». *Information Ethics*. Universidad de Alberta. [https://www.academia.edu/4896164/Information\\_Ethics\\_II\\_Towards\\_a\\_Unified\\_Taxonomy](https://www.academia.edu/4896164/Information_Ethics_II_Towards_a_Unified_Taxonomy) [Fecha de consulta: 28 de marzo de 2016].

**Carmody, T.** (2010, 20 de noviembre). «You are not your name and photo, a call to re-imagine identity». WIRED. <https://www.wired.com/2011/10/you-are-not-your-name-and-photo-a-call-to-re-imagine-identity/> [Fecha de consulta: 8 de diciembre de 2016].

**Dull, T.** (2015). «Big data and the Internet of Things: Two sides of the same coin?». *SAS best practices*. [http://www.sas.com/en\\_us/insights/articles/big\\_data/big\\_data-and-iot-two-sides-of-the-same-coin.html](http://www.sas.com/en_us/insights/articles/big_data/big_data-and-iot-two-sides-of-the-same-coin.html) [Fecha de consulta: 21 de diciembre de 2015].

**Helft, M.** (2011, 13 de mayo). «Facebook, foe of anonymity, is forced to explain a secret». *The New York Times*. <http://www.nytimes.com/2011/05/14/technology/14facebook.html> [Fecha de consulta: 8 de diciembre de 2016].

**Massachusetts Institute of Technology (MIT).** *Moral Machine Project*. <http://moralmachine.mit.edu/> [Fecha de consulta: 21 de noviembre de 2016].

**Observatori de Bioètica y Dret de la Universitat de Barcelona.** *El informe Belmont*. <http://www.bioeticayderecho.ub.edu/archivos/norm/InformeBelmont.pdf> [Fecha de consulta: 24 de noviembre de 2016].

**The good Project.** <http://www.thegoodproject.org/projects/the-good-work-project/> [Fecha de consulta: 30 de octubre de 2016].

**The Guardian.** *The Snowden Files*. Recopilación de documentos relacionados con las revelaciones de Snowden. <https://www.theguardian.com/world/series/the-snowden-files> [Fecha de consulta: 9 de diciembre de 2016].

**Washington D.C.: Department of Health, Education, and Welfare.** *The Belmont Report: Ethical Guidelines for the Protection of Human Subjects of Research*. <http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/> [Fecha de consulta: 24 de noviembre de 2016].