PRIVACIDAD ES PODER



DATOS, VIGILANCIA Y LIBERTAD EN LA ERA DIGITAL

CARISSA VÉLIZ

DEBATE

Privacidad es poder

Datos, vigilancia y libertad en la era digital

CARISSA VÉLIZ

DEBATE

A mi madre, tierra firme que me dio alas

Introducción

Nos vigilan. Saben que estoy escribiendo estas palabras. Saben que las estás leyendo. Gobiernos y cientos de empresas nos espían: a ti, a mí y a todos nuestros conocidos. Cada minuto, todos los días. Rastrean y registran todo lo que pueden: nuestra ubicación, nuestras comunicaciones, nuestras búsquedas en internet, nuestra información biométrica, nuestras relaciones sociales, nuestras compras y mucho más. Quieren saber quiénes somos, qué pensamos, dónde nos duele. Quieren predecir nuestro comportamiento e influir en él. Tienen demasiado poder. Su poder proviene de nosotros, de ti, de tus datos. Es hora de volver a tomar el control. Recuperar la privacidad es la única manera de que podamos asumir de nuevo el mando de nuestra vida y de nuestras sociedades.

Internet se financia principalmente mediante la recopilación, el análisis y el comercio de datos: la economía de los datos. Muchos de ellos son personales: datos sobre ti. La compraventa de estos datos personales como modelo de negocio se está exportando a cada vez más instituciones de la sociedad, que pasa a ser la sociedad (o el capitalismo) de la vigilancia. [1]

Para llegar a ti, tuve que pasar por el capitalismo de la vigilancia; lo siento. [2] ¿Cómo llegaste a tener conocimiento de este libro? ¿Recuerdas cómo te enteraste por primera vez de que existía, o dónde lo viste anunciado? Tal vez te etiquetaran en alguna plataforma como una persona «pionera», alguien que está siempre pendiente de conocer y experimentar cosas nuevas, alguien a quien le gustan los libros que le hacen pensar. O quizá seas alguien «sensibilizado»: una persona preocupada por temas sociales e interesada por la política. ¿Encajas en el perfil? El principal objetivo de este libro es empoderarte, pero la mayoría de los usos que se hacen de tus datos te desempoderan.

Si la vigilancia no te atrapó antes de que compraras este libro, es probable que lo haya hecho después. Si estás leyendo estas líneas en un dispositivo con Kindle, Google Books o Nook, están midiendo cuánto tardas en leer cada palabra, dónde te detienes para hacer una pausa y qué resaltas. Si adquiriste el libro en una librería, el teléfono inteligente que llevabas en el bolsillo se encargó de registrar tu trayecto hasta allí y cuánto tiempo estuviste en la tienda. [3] Puede que la música que sonaba en la librería estuviera enviando balizas ultrasónicas a tu teléfono para identificarlo como *tu* aparato y rastrear así lo que te interesa y lo que compras. Si utilizaste una tarjeta de débito o de crédito para comprar el libro, probablemente alguien vendió esos datos a brókeres de datos

que luego los revendieron a compañías aseguradoras, potenciales empleadores, gobiernos, empresas y cualesquiera otros a quienes pudieran interesarles. O tal vez alguien haya enlazado tu tarjeta de pago con un sistema de fidelización como cliente que hace un seguimiento de tu historial de compras y usa esa información para mostrarte más cosas que, según el algoritmo, a lo mejor podrías comprar.

La economía de los datos, y la vigilancia omnipresente de la que se nutre, nos pillaron desprevenidos. Las compañías tecnológicas no informaron a los usuarios de cómo utilizan nuestros datos ni, menos aún, nos pidieron permiso para usarlos. Tampoco se lo solicitaron a nuestros gobiernos. No había leyes que regularan el rastro de los datos que los confiados ciudadanos dejábamos mientras nos ocupábamos de nuestras cosas en un entorno cada vez más digitalizado. Cuando nos dimos cuenta de lo que ocurría, la arquitectura de la vigilancia estaba ya instalada. Buena parte de nuestra privacidad había desaparecido. A raíz de la pandemia de coronavirus, la privacidad se ha visto enfrentada a nuevas amenazas, pues ahora realizamos en línea muchas actividades que antes estaban fuera del mundo digital, y se nos pide que entreguemos nuestros datos personales en aras del bien común. Va siendo hora de que reflexionemos muy en serio sobre el tipo de mundo en el que querremos vivir cuando la pandemia se convierta en un recuerdo lejano. Un mundo sin privacidad es un mundo peligroso.

La privacidad consiste en no compartir con otros ciertas cuestiones íntimas: nuestros pensamientos, nuestras experiencias, nuestras conversaciones, nuestros planes. Los seres humanos necesitamos privacidad para poder relajarnos de la carga que supone estar con otras personas. Necesitamos privacidad para explorar ideas nuevas con libertad, para formarnos nuestra propia opinión. La privacidad nos protege de las presiones no deseadas y abusos de poder. La necesitamos para ser individuos autónomos, y las democracias solo pueden funcionar bien cuando los ciudadanos gozamos de autonomía.

Nuestras vidas, traducidas en datos, son la materia prima de la economía de la vigilancia. Nuestras esperanzas, nuestros miedos, lo que leemos, lo que escribimos, nuestras relaciones, nuestras enfermedades, nuestros errores, nuestras compras, nuestras debilidades, nuestros rostros, nuestras voces... todo sirve de carroña para los buitres de datos que lo recopilan todo, lo analizan todo y lo venden al mejor postor. Muchos de los que adquieren nuestros datos los quieren para fines perversos: para delatar nuestros secretos a las compañías aseguradoras, a los empleadores y a los gobiernos; para vendernos cosas que no está en nuestro interés comprar; para enfrentarnos unos contra otros en un intento de destruir nuestra sociedad desde dentro; para desinformarnos y

secuestrar nuestras democracias. La sociedad de la vigilancia ha transformado a los *ciudadanos* en *usuarios* y en *sujetos de datos* . Ya basta. Quienes han violado nuestro derecho a la privacidad han abusado de nuestra confianza y es hora de que los desenchufemos de su fuente de poder: nuestros datos.

Es demasiado tarde para impedir que se desarrolle la economía de los datos, pero no es demasiado tarde para recuperar nuestra privacidad. Nuestros derechos civiles están en juego. Las decisiones que tomemos sobre la privacidad hoy y en los próximos años moldearán durante décadas el futuro de la humanidad. Las elecciones de la sociedad en materia de privacidad influirán en cómo se desarrollarán las campañas políticas, cómo se ganarán su sustento las grandes empresas, cuál será el poder que los gobiernos y las compañías privadas serán capaces de ejercer, cómo progresará la medicina, cómo se perseguirán los objetivos de salud pública, cuáles serán los riesgos a los que estaremos expuestos, cómo interactuaremos unos con otros y, en no menor medida, si se respetarán nuestros derechos mientras nos ocupamos de nuestros quehaceres cotidianos.

Este libro trata del estado actual de la privacidad, de cómo se creó la economía de la vigilancia, de por qué debemos poner fin al comercio de datos personales y de cómo hacerlo. El capítulo 1 acompaña a una persona a lo largo de su jornada en la sociedad de la vigilancia para ilustrar cuánta privacidad se nos está robando. El capítulo 2 explica cómo se desarrolló la economía de los datos, y lo hace con la esperanza de que entender cómo nos metimos en este lío nos ayude a salir de él. En el capítulo 3 sostengo que la privacidad es una forma de poder y que quien posea más datos personales dominará la sociedad. Si damos nuestros datos a las empresas privadas, mandarán los ricos. Si se los damos a los gobiernos, terminaremos sufriendo alguna forma de autoritarismo. Solo si las personas conservan sus datos la sociedad será libre. La privacidad importa porque da poder a la ciudadanía.

La economía de la vigilancia no solo es mala porque genera y potencia unas asimetrías de poder nada aconsejables; es también peligrosa porque comercia con una sustancia tóxica. El capítulo 4 examina por qué los datos personales son tóxicos y cómo están envenenando nuestras vidas, nuestras instituciones y nuestras sociedades. Tenemos que poner freno a la economía de los datos igual que se lo pusimos a otras formas de explotación económica en el pasado. Los sistemas económicos que dependen de la vulneración de derechos son inaceptables. El tema del capítulo 5 es cómo podemos desenchufar el cable que alimenta a la economía de la vigilancia. El del capítulo 6 es qué puedes hacer tú, como individuo, para asumir de nuevo el control de tus datos personales y de nuestras democracias.

No estamos asistiendo a la muerte de la privacidad. Aunque la privacidad corre peligro, estamos mejor situados para defenderla hoy de lo que lo hemos estado durante la última década. Este es solo el comienzo de la lucha por salvaguardar los datos personales en la era digital. Hay demasiado en juego como para dejar que la privacidad se marchite; nuestra propia forma de vida está en riesgo. La vigilancia amenaza la libertad, la igualdad, la democracia, la autonomía, la creatividad y la intimidad. Se nos ha mentido una y otra vez, y nos están robando nuestros datos para usarlos contra nosotros. No más. Tener demasiada poca privacidad es incompatible con el buen funcionamiento de una sociedad libre. El capitalismo de la vigilancia tiene que desaparecer. Harán falta tiempo y esfuerzo, pero podemos recuperar la privacidad y la recuperaremos. He aquí cómo.

1

Buitres de datos

Si estás leyendo este libro, es probable que ya sepas que tus datos personales se recopilan, se guardan y se analizan. Pero ¿eres consciente del alcance al que llegan las invasiones de la privacidad en tu vida? Empecemos por el amanecer.

¿Qué es lo primero que haces cuando te despiertas por la mañana? Probablemente, miras tu teléfono. *Voilà* ! Ese es el primer dato que pierdes en el día. Al coger tu teléfono a primera hora de la mañana estás informando a toda una serie de entrometidos —el fabricante de tu móvil, todas las aplicaciones que tienes instaladas en él, tu compañía de teléfono, así como las agencias de inteligencia, si resultas ser una persona «de interés»— de a qué hora te despiertas, dónde has dormido y con quién (suponiendo que la persona con quien compartes cama también tenga su propio teléfono cerca).

Si llevas puesto un reloj inteligente en la muñeca, habrás perdido algo de tu privacidad incluso antes de despertarte, pues este habrá registrado todos tus movimientos en la cama (incluida, desde luego, cualquier actividad sexual). [1] Supongamos que tu empresa te dio ese reloj como parte de un programa pensado para incentivar hábitos saludables y para, de ese modo, pagar primas más baratas por los seguros de sus trabajadores. ¿Puedes estar segura de que tus datos no se utilizarán en tu contra, o de que tu jefe no los verá? [2] Cuando tu empresa te da un dispositivo, es ella la que continúa siendo dueña legal de este —tanto da si es un aparato de registro de actividad física, un ordenador portátil o un teléfono— y puede acceder a los datos en él registrados en cualquier momento y sin tu permiso. [3]

Después de mirar cuál ha sido tu frecuencia cardiaca durante la noche (demasiado rápida, necesitas hacer más ejercicio) y enviar esos datos a tu teléfono móvil, te levantas de la cama y te lavas los dientes con un cepillo eléctrico. Una app te informa de que no te los lavas tan a menudo como deberías.

Esta mañana se te han pegado las sábanas y tu pareja se ha ido ya a trabajar. Vas a la cocina y buscas azúcar para el café, pero te das cuenta de que no queda. Decides preguntarle a la vecina si le sobra un poco. Cuando estás frente a su puerta, percibes algo inusual, una cámara. Tu vecina te lo explica nada más abrir: es un nuevo timbre inteligente. Se trata de un aparato de la casa Ring, una empresa de Amazon. Es muy probable que los empleados de Ring revisen luego

ese vídeo que se ha grabado de ti para etiquetar objetos manualmente a fin de entrenar a su software para realizar tareas de reconocimiento. Esos vídeos se almacenan sin cifrar, lo que los hace extraordinariamente vulnerables al jaqueo. [4] Amazon ha presentado una solicitud de patente para el uso de su software de reconocimiento facial en timbres. Nest, propiedad de Google, ya utiliza el reconocimiento facial en sus cámaras. En algunas ciudades, como Washington, la policía quiere llevar un registro oficial de todas las cámaras de seguridad privadas e incluso subvencionarlas. [5] A saber dónde irán a parar las grabaciones de esos timbres inteligentes y para qué se usarán.

Tu vecina no tiene azúcar (o tal vez no quiera dártelo después de que le hayas hecho el feo a su nuevo timbre). Te vas a tener que conformar con beberte el café sin endulzar. Enciendes el televisor (inteligente, por supuesto) para distraerte de ese amargor en la boca. Están poniendo tu programa favorito: ese placer culpable que jamás admitirás que ves.

Te llaman. Es tu pareja. Silencias el televisor.

—¿Aún en casa? —pregunta.

—Y tú ¿cómo lo sabes?

—Mi teléfono está conectado a nuestro contador inteligente. He visto que estabas consumiendo electricidad.

—Me he dormido —admites entonces.

No parece muy convencido por tu explicación, pero tiene una reunión y debe colgar.

Te preguntas si no te habrán espiado más veces por medio de tu contador inteligente. Estos aparatos no solo constituyen un riesgo para la privacidad de los individuos con respecto a las personas con quienes comparten domicilio, sino que también se ha constatado que son dispositivos muy inseguros. [6] Un delincuente puede jaquearte el tuyo y ver cuándo no estás en casa para entrar a robar. [7] Además, los datos de los contadores inteligentes se conservan y se analizan en los ordenadores de las compañías proveedoras. Algunos de esos datos pueden ser bastante sensibles. Por ejemplo, tu huella energética es tan precisa que puede revelar hasta qué canal de televisión estás viendo. [8] Esos datos pueden venderse o compartirse con terceros.

Tu hijo adolescente entra en la cocina e interrumpe tus pensamientos. Quiere hablar contigo de algo delicado. Puede que sea un problema relacionado con drogas, sexo o un tema de acoso escolar. No apagas el televisor inteligente; aunque silenciado, este sigue emitiendo imágenes de fondo. Es probable que tu televisor esté recopilando información mediante una tecnología llamada «reconocimiento automático de contenido» (ACR, por sus siglas en inglés), que trata de identificar todo lo que ves por televisión y envía los datos al fabricante

del aparato, a terceros, o a ambos. Unos investigadores descubrieron que un televisor inteligente de la casa Samsung se había conectado a más de setecientas direcciones de internet después de solo quince minutos de uso. [9]

Eso es lo de menos. Si tuvieras tiempo para leerte las políticas de privacidad de los aparatos que compras, te habrías dado cuenta de que tu televisor Samsung incluía la siguiente advertencia: «Tenga en cuenta que, si entre las palabras que dice se incluye información personal o sensible, esta se encontrará entre los datos recopilados y transmitidos a terceros». [10] Incluso cuando crees que has apagado el televisor, es posible que siga encendido. Agencias de inteligencia como la CIA o el MI5 pueden hacer que parezca que tu televisor está apagado mientras graba lo que dices. [11]

Después de haber compartido sus preocupaciones más íntimas contigo (y con el fabricante de tu televisor, y con cientos de terceros desconocidos), tu hijo se va al instituto, donde perderá más privacidad debido a la vigilancia escolar de su uso de internet. [12] Mientras tanto, vuelves a activar el sonido del televisor. Están pasando anuncios. Si piensas que por fin vas a tener un momento de privacidad, te equivocas. Sin que te des cuenta, esos anuncios televisivos están emitiendo unas balizas sonoras inaudibles (como también las emiten mucha de la publicidad radiofónica o de la música de ambiente en las tiendas) que recibe tu teléfono. Estas balizas de audio funcionan como *cookies* sonoras que permiten que las empresas triangulen nuestros dispositivos y hábitos de compra a partir de nuestra ubicación. Dicho de otro modo, ayudan a los vendedores a seguirte el rastro a través de tus diferentes dispositivos. Gracias a este rastreo ultrasónico, una empresa puede saber si la persona que ve un anuncio de un producto por la mañana en la televisión y lo busca en su portátil una hora después va luego a comprarlo a la tienda de su barrio o lo encarga en línea. [13]

Recibes otra llamada. Esta vez es de un compañero de trabajo.

—Oye, no estoy seguro de cómo ha pasado, pero acabo de recibir una grabación de una conversación muy privada que estabas teniendo con tu hijo. Parece que la ha enviado tu asistente digital Alexa.

Le agradeces que te lo haya dicho y cuelgas. ¿Habrá enviado Alexa esa conversación a otras personas de tu lista de contactos? Furiosa, te pones en contacto con Amazon. Te explican: «Es probable que Echo se activara con alguna palabra de su conversación que sonó parecida a “Alexa”. Y que luego pensara que le estaba diciendo “enviar mensaje”. Seguramente, preguntó entonces “¿A quién?”, e interpretó un nombre a partir de algo que alguno de ustedes dijo en ese momento». [14] Hay veces en que los altavoces inteligentes se despiertan al oír que, en un programa de televisión, se dice algo parecido a su palabra de activación. Si tuvieras la televisión encendida todo el rato, eso

ocurriría entre una y media y diecinueve veces al día (sin contar las ocasiones en que se dice realmente la palabra de activación). [15] Cuando Alexa envió la conversación privada de un usuario de Portland (Oregón) a uno de sus contactos, aquel prometió no volver a conectarse al dispositivo nunca más. [16] Tú vas un paso más allá y estampas el Echo contra la pared. A tu pareja no le va a hacer ninguna gracia.

Se te ha hecho tarde para llegar al trabajo. Subes a tu coche y lo conduces hasta la oficina. Es un vehículo que compraste de segunda mano a una conocida. Probablemente no se te haya pasado nunca por la cabeza, pero resulta que esa persona tiene acceso a tus datos porque nunca desconectó su teléfono de la aplicación del automóvil. [17] Además, el fabricante del vehículo recopila toda clase de datos sobre ti —los lugares que visitas, la velocidad a la que circulas, tus gustos musicales, tus movimientos oculares, si llevas las manos al volante o no, y hasta tu peso (medido por tu asiento)—, datos que pueden, todos ellos, terminar en manos de tu compañía aseguradora, entre otros terceros. [18]

Llegas al trabajo. Vives en Londres y tu oficina está en Westminster. Al pasar junto al edificio del Parlamento, puede que tus datos del teléfono sean aspirados por unos receptores IMSI (conocidos asimismo como «mantarrayas», que son torres de telefonía simuladas que engañan a los móviles para que se conecten a ellas). Los receptores IMSI recopilan datos de identificación y ubicación. También permiten espiar conversaciones telefónicas, mensajes de texto y navegación por internet. [19] Según la Unión Estadounidense por las Libertades Civiles (ACLU, por sus siglas en inglés), en Estados Unidos, al menos 75 organismos y cuerpos gubernamentales de veintisiete estados disponen de esa tecnología (aunque puede que sean muchos más y no lo sepamos). [20] Según un artículo publicado en *The Intercept* , las agencias de seguridad en ocasiones han «engañado a jueces» y han «confundido a abogados defensores» sobre su uso de dispositivos mantarrayas, diciendo, por ejemplo, que obtuvieron información relevante sobre un acusado a partir de una «fuente confidencial», cuando en realidad se valieron de un receptor IMSI. [21]

Algunos activistas creen que es probable que se hayan usado mantarrayas contra manifestantes del movimiento Black Lives Matter en Estados Unidos en el 2020. [22] Hay pruebas de que la policía está utilizando estos equipos en Londres para espiar a personas, por ejemplo en manifestaciones pacíficas o en las inmediaciones del Parlamento británico. [23] Un consejo que se da en los foros digitales para proteger tu privacidad es que dejes el teléfono en casa cuando vayas a una manifestación; pero el móvil es importante durante una protesta para mantenerte en contacto con tus conocidos y al tanto de la información relevante. Aunque las mantarrayas son usadas sobre todo por los

gobiernos, cualquiera puede adquirirlas, ya que son productos comercializados por empresas privadas, y también los hay de fabricación casera.

Mientras te están aspirando los datos del teléfono, entras en tu oficina. Un compañero te saluda y mira su reloj, dejando claro que tu retraso no ha pasado desapercibido. Te sientas frente al ordenador e intentas respirar hondo, pero te falta el aire al ver que tienes cientos de correos electrónicos sin leer. [24] Abres el primero. Es de tu jefe: «Hola, he visto que no estabas en la oficina esta mañana. ¿Tendrás listo a tiempo el informe que te pedí?». Sí, lo tendrás, pero desearías que tu jefe no estuviera agobiándote.

El siguiente correo te pide que rellenes un formulario con unas evaluaciones anónimas de tus compañeros de trabajo. Tu jefe es un firme defensor de la vigilancia laboral. Sabes que supervisa hasta el último movimiento que haces y que controla si vas a las reuniones, a los seminarios y hasta a las cenas y salidas de copas informales después del trabajo. Sabes que monitoriza tus redes sociales porque ya te ha advertido en el pasado sobre publicar contenidos políticos. Se te revuelve el estómago ante la idea de evaluar a tus colegas y que ellos te evalúen.

A continuación, aparece un correo de tu marca de zapatos favorita. Tal vez creas que recibir correos es inocuo para tu privacidad, pero alrededor del 70 por ciento de los correos comerciales (y un 40 por ciento del total) contienen rastreadores. [25] Abrir uno de esos mensajes permite que otros rastreen tu actividad por la web y te identifiquen como usuaria única, aunque navegues desde dispositivos diferentes. Se pueden insertar rastreadores en un color, un tipo de letra, un píxel o un enlace. Hasta los usuarios corrientes incluyen rastreadores para saber si sus correos se leen (y cuándo y dónde). Dado que los rastreadores pueden revelar la ubicación de una persona, un acosador podría utilizarlos para encontrarte.

El siguiente mensaje de correo es de tu hermano. Te lo ha enviado a tu cuenta del trabajo, aunque le hayas pedido mil veces que no use esa cuenta. Las empresas y organizaciones (incluidas las universidades) tienen acceso a los correos electrónicos de sus empleados [26] (una razón más para no usar nunca la cuenta del trabajo para asuntos personales). En su mensaje, tu hermano te informa de que, por su cumpleaños, le regalaron un kit comercial de pruebas genéticas para particulares y decidió hacerse la prueba. Tal vez te guste saber, escribe en su mensaje, que la familia tiene un 25 por ciento de ascendencia italiana. La mala noticia es que le dicen que presenta un 30 por ciento de probabilidades de padecer una enfermedad cardiaca; como es tu hermano, esa probabilidad, a su vez, es la tuya. Tú le respondes: «Ojalá me hubieras pedido permiso antes. También son mis genes y los de mi hijo. ¿No sabías que nuestra abuela era italiana? Si quieres saber más sobre nuestra familia, pregúntame».

Preocupada por tus datos genéticos, lees la política de privacidad de la compañía cuyos servicios utilizó su hermano. No tiene buena pinta. Las compañías que realizan las pruebas pueden considerarse propietarias de la muestra de ADN que se les envíe y usarla como deseen. [27] Las políticas de privacidad de las empresas de análisis de ADN suelen incluir referencias a la «desidentificación» o «seudonimización» de la información para tranquilizar a los usuarios. No obstante, es difícil «desidentificar» unos datos genéticos. Por su propia naturaleza, los datos genéticos permiten identificar a los individuos y a sus conexiones familiares. Sustituir los nombres por unos números identificativos generados al azar no proporciona mucha protección contra la reidentificación. En 2000, los informáticos Bradley Malin y Latanya Sweeney reidentificaron entre el 98 y el 100 por ciento de los individuos en una base de datos de ADN «anonimizada» valiéndose de datos sanitarios personales que estaban disponibles al público y de conocimientos sobre enfermedades concretas. [28]

Te preguntas en dónde acabarán los datos genéticos de tu hermano y si alguna vez se usarán en contra de ti o de tu hijo al solicitar un seguro o un empleo, por ejemplo. Lo peor de todo es que las pruebas genéticas comerciales son muy imprecisas. Alrededor del 40 por ciento de los resultados son falsos positivos. [29] Tu hermano puede haber regalado toda la privacidad genética de la familia a cambio de un informe lleno de palabrería barata que, sin embargo, las compañías de seguros y otras instituciones interpretarán como hechos demostrados.

En cualquier caso, ahora te toca hacer una videollamada de trabajo a un cliente que te ha pedido que os conectéis por Zoom. Muchas personas no habían oído hablar de Zoom antes de la pandemia de coronavirus, cuando se convirtió en la aplicación de videoconferencias más popular. Durante el confinamiento, te horrorizaste al enterarte de las toneladas de datos que Zoom recopilaba de ti, entre ellos, tu nombre, tu ubicación física, tu dirección de correo electrónico, tu cargo profesional, tu empresa, tu dirección de IP (y muchos más). [30] Te han llegado noticias de que Zoom ha mejorado por fin sus políticas de privacidad y seguridad, pero ¿puedes fiarte de una compañía que aseguraba haber puesto en práctica un sistema de cifrado de extremo a extremo cuando, en realidad, no lo había hecho? [31]

Concluida la llamada, y para relajarte un poco, te conectas a Facebook. Solo un momentito, te dices. Quizá te animes viendo las fotos de tus amigos pasándoselo bien (te vas a desanimar). Como sospechas que tu jefe monitoriza lo que haces en el ordenador, utilizas tu teléfono personal.

Facebook ha vulnerado nuestro derecho a la privacidad tantas veces que repasarlas nos llevaría otro libro entero. Aquí mencionaré solamente algunas de

las formas en las que invade nuestra privacidad.

Todo lo que haces mientras estás conectada a Facebook se rastrea, desde tus movimientos con el ratón [32] hasta aquello que escribes y luego decides borrar antes de publicarlo (tu autocensura). [33] Empiezas navegando por la sección titulada «Personas que quizá conozcas». Se trata de una función que tuvo un papel crucial en la expansión de Facebook como red social, cuando pasó de los 100 millones de miembros que tenía en 2008 (cuando se introdujo la mencionada herramienta) a más de 2.000 millones en 2018. Entre las personas a las que puedes ver allí, tal vez reconozcas a parientes lejanos, o a antiguos compañeros de colegio. No parece que haya nada de malo en ello, ¿no? Te recomiendo que no te metas mucho más a fondo en esa madriguera. Si lo haces, es probable que acabes por darte cuenta de que Facebook está intentando conectarte con personas con quienes no quieres tener contacto.

Algunas conexiones entre personas son problemáticas; es el caso, por ejemplo, de cuando se expone la identidad real de trabajadores o trabajadoras sexuales a sus clientes. [34] O de cuando la plataforma vincula entre sí a pacientes de una misma psiquiatra y compromete la confidencialidad médica. La psiquiatra en cuestión no se había hecho amiga de sus pacientes en Facebook, pero estos probablemente la tenían en sus respectivas libretas de contactos. [35] Entre otras muchas desafortunadas conexiones, Facebook también ha sugerido a un acosador como «amigo» a su víctima (hasta entonces anónima), a un marido al amante de su mujer, y a alguien a quien le habían robado el coche al ladrón del vehículo. [36]

Según su declaración de objetivos, la misión de Facebook es «ofrecer a las personas el poder de crear comunidades y hacer del mundo un lugar más conectado». ¿Y qué hay de dar a las personas el poder de *desconectarse* de relaciones tóxicas o indeseables? «Hacer del mundo un lugar más conectado» suena muy amigable hasta que te preguntas si quieres que se te obligue a tener tal conexión con personas que te caen mal, a quienes temes o que deseas tener lejos por razones profesionales o personales.

Facebook ha demostrado su falta de respeto por la privacidad de muchas otras formas. La empresa Cambridge Analytica analizó los datos de unos 87 millones de usuarios de la red social con fines políticos. [37] En 2018, le robaron los datos personales a 14 millones de usuarios a raíz de un jaqueo. [38] Durante años, Facebook permitió que el motor de búsqueda Bing de Microsoft viera los amigos de los usuarios de la red social sin el consentimiento de estos, y dio a Netflix y a Spotify la capacidad de leer y hasta de borrar mensajes «privados» de usuarios de Facebook. [39] En 2015, comenzó a registrar todos los mensajes de texto y llamadas de usuarios de Android sin haberles pedido permiso. [40]

Es probable que Facebook haya usado el reconocimiento facial con las fotos que has colgado en su red sin haber obtenido antes tu debido consentimiento. Cuando Facebook te sugirió etiquetar a tus amigos y aceptaste, lo que hiciste fue ceder gratis tanto la privacidad de tus relaciones como tu mano de obra para entrenar al algoritmo de reconocimiento facial. Facebook ha presentado solicitudes de patentes en las que se describen sistemas para reconocer rostros de los compradores en las tiendas y hacerlos corresponder con sus perfiles en redes sociales. [41] Por si eso fuera poco, Facebook también pidió a los usuarios sus números de teléfono como medida de seguridad y luego aprovechó esa información para sus propios fines: concretamente, para crear publicidad dirigida y unificar sus conjuntos de datos con los de WhatsApp, su aplicación de mensajería. [42] En 2019, se filtraron cientos de millones de números de teléfono de usuarios de Facebook en una base de datos abierta en línea porque el servidor en el que se guardaban no estaba protegido con contraseña. [43]

El último escándalo es que los datos de 533 millones de usuarios de Facebook (incluyendo número de teléfono y datos de localización) han sido publicados en línea en una página para jáqueres. [44] Con esos datos, es muy fácil saber dónde vive una persona, robarle la identidad, y más. El colmo de los colmos fue que Facebook dio a entender que la culpa era de los usuarios por no configurar sus cuentas a opciones más privadas. [45] Estos son solo algunos de los desastres más recientes, pero la lista completa es larga y todo parece indicar que las violaciones de nuestro derecho a la privacidad por parte de Facebook no van a parar. [46]

Facebook puede parecer una red social, pero su verdadero negocio consiste en la compraventa de influencia a través de los datos personales. Tiene más de plataforma de publicidad personalizada que de medio social. Está dispuesta a llegar muy lejos con tal de arañar tantos datos personales como sea posible con la mínima fricción, para luego poder vender a los anunciantes el acceso a la atención de sus usuarios. La historia de Facebook nos muestra que, si puede salir impune sin pedir consentimiento —como, hasta el momento, ha sucedido—, no lo solicita, como tampoco se esfuerza por investigar quién recibe los datos de sus usuarios ni cómo se utilizan, y no tiene reparos en incumplir sus promesas. [47] Proteger tu privacidad parece estar en el puesto más bajo de su lista de prioridades. Y ni siquiera puedes mantenerte al margen de este monstruo hambriento de datos, porque Facebook elabora perfiles «sombra» de ti, aunque nunca hayas usado su plataforma. Te sigue por la web a través de sus omnipresentes iconos de «me gusta», y lo hace incluso aunque no hagas clic en ellos. [48] No es de extrañar, pues, que en un informe del Parlamento británico se dijera que Facebook se ha comportado como un «gánster digital» en estos

últimos años. [49]

Tras navegar por Facebook un rato y sentir escalofríos por las amistades que te sugiere y los anuncios que te muestra, decides tomarte un descanso. Intentas ponerte a trabajar, pero no logras concentrarte; te agobia la idea de que tu jefe está monitorizando todo lo que haces en el ordenador. Por suerte, es la hora del almuerzo. Pero no tienes hambre, así que optas por acercarte a una tienda para comprarle algo a tu hijo para animarlo un poco.

Entras en una tienda de ropa en busca de una camisa. Los comercios físicos se han sentido desfavorecidos con respecto a los electrónicos, porque estos últimos fueron los primeros en recabar datos de los clientes. Ahora están intentando recuperar el terreno perdido. La tienda en la que entras utiliza una tecnología que te identifica como cliente recurrente gracias a la señal wifi de tu móvil (por eso hay que apagar el wifi cuando salgas de casa). Los dispositivos móviles envían códigos de identificación específicos (las llamadas direcciones MAC) cuando buscan redes con las que conectarse a la web. Las tiendas usan esa información para estudiar tu comportamiento. [50]

No contentos con ello, los comercios pueden emplear también cámaras para recopilar más datos sobre ti. Estos aparatos pueden cartografiar tu recorrido por la tienda y estudiar qué te atrae. Las cámaras han adquirido tal nivel de sofisticación que pueden analizar qué estás mirando y hasta cuál es tu estado de ánimo basándose en tu lenguaje corporal y expresión facial. [51] Es posible que el establecimiento también esté utilizando reconocimiento facial, el cual, entre otros usos, posibilita las referencias cruzadas entre tu rostro y una base de datos en la que se busca alguna correspondencia con antiguos ladrones o delincuentes conocidos. [52]

Sales de la tienda y miras el teléfono. Una alerta te recuerda que tienes cita con el médico. Hay un problema de salud que te inquieta desde hace algunas semanas. Has buscado información en línea tratando de encontrar una solución y también has esperado que desapareciera por sí solo, pero no lo ha hecho. No se lo has dicho a nadie en la familia para no causar una preocupación innecesaria. Nuestros motores de búsqueda saben más de nosotros que nuestras parejas; nunca les mentimos ni les ocultamos nuestras inquietudes.

Vas al médico. Mientras estás en la sala de espera, recibes una notificación. Tu hermana ha publicado la foto más reciente de tu sobrinita, aún bebé. Sus manitas rechonchas te hacen sonreír. Tomas nota mental de no olvidarte de advertir a tu hermana de los riesgos de exponer a sus hijos pequeños en línea. Deberías decirle que nuestras fotografías en la red se utilizan para entrenar a algoritmos de reconocimiento facial que luego se usan para toda clase de fines perversos: desde la vigilancia a la que los regímenes autoritarios someten a poblaciones

vulnerables, hasta la divulgación de la identidad de actrices y actores pornográficos, y la identificación de personas en lugares como el metro en Rusia. [53] Pero la irresistible sonrisa de tu sobrina te distrae. Sus fotos son, a veces, lo mejor de tu día, la golosina que endulza el regusto amargo que la economía de los datos deja en ti, aunque sepas que es precisamente de contenidos cautivadores como las fotos de bebés adorables de lo que se alimentan los buitres de datos.

Una enfermera te avisa de que la doctora ya puede verte. Tu médica te hace ciertas preguntas delicadas, va escribiendo tus respuestas en el ordenador y te programa unas pruebas, y tú mientras tanto te preguntas adónde podría ir a parar esa información. Muchas veces, tus datos médicos están en venta. Los brókeres de datos [54] —que se dedican a comerciar con datos personales— pueden adquirirlos de farmacias, hospitales, consultas de doctores, apps médicas y búsquedas de internet, entre otras fuentes. Tus datos médicos pueden ir a parar también a manos de investigadores, aseguradoras o empleadores potenciales. [55]

Un sistema nacional sanitario como el británico (NHS, por sus siglas en inglés) podría decidir donar tu historial médico a una empresa como DeepMind, propiedad de Alphabet (compañía matriz de Google). Esa transferencia de datos podría efectuarse sin tu consentimiento, sin que obtengas beneficio alguno de semejante invasión de tu privacidad, y sin ninguna garantía legal de que DeepMind no vaya a vincular tus datos personales con tu cuenta de Google y, con ello, erosione aún más tu privacidad. [56] En 2019, se interpuso una demanda judicial colectiva contra la Universidad de Chicago y Google. En ella se acusaba al hospital de dicha institución educativa de estar compartiendo con la tecnológica cientos de miles de historiales de los pacientes sin borrar sellos de fecha identificables ni notas de los médicos. A Google se le acusaba de «enriquecimiento ilícito». [57]

También podrías ser víctima de un robo de datos. En 2015, solo en Estados Unidos, más de 112 millones de historiales médicos se filtraron indebidamente. [58] Incluso podrían extorsionarte. En 2017, unos delincuentes lograron acceder a historiales médicos de una clínica y chantajearon a los pacientes; terminaron publicando miles de fotos privadas (algunas de desnudos) y datos personales, entre los que se incluían pasaportes escaneados y números de la seguridad social. [59]

Mientras estos pensamientos te revolotean por la cabeza, te sientes tentada de mentir a tu médica a propósito de cierta información delicada que tal vez (esperas) no sea necesaria para que te dé un diagnóstico preciso. Puede que incluso optes por no hacerte las pruebas que te ha indicado, aunque te hagan

falta.

Tras la visita con la doctora, vuelves a casa para hacer la maleta para un viaje de trabajo a Estados Unidos. Las apps de tu teléfono han ido rastreando toda tu jornada. Si permites que los servicios de ubicación estén activos para poder recibir noticias, pronósticos meteorológicos y otra información de carácter local, decenas de compañías reciben datos de ubicación sobre ti. En algunos casos, esas aplicaciones actualizan y recopilan tus datos de ubicación más de 14.000 veces al día. La publicidad dirigida según la ubicación mueve unas cifras de negocio que se estiman en más de 17.500 millones de euros anuales. [60]

Entre los muchos agentes que venden tus datos de ubicación se encuentran las telecos. Celosas del éxito del negocio de Silicon Valley, las empresas de telecomunicaciones están ansiosas por competir en el mercado del comercio de datos. [61] Tu móvil está conectándose constantemente a la torre de telefonía más próxima. Por eso, tu compañía telefónica sabe siempre dónde te encuentras. [62] Las redes móviles no solo venden datos de ubicación a otras empresas; algunos periodistas han revelado que, como mínimo, ciertos proveedores de servicio de telefonía móvil también están vendiendo datos de los usuarios en el mercado negro. La conclusión es que cualquiera que tenga un móvil es susceptible de ser vigilado por acosadores, delincuentes, agentes de los cuerpos de seguridad (de cualquier rango y sin orden judicial de por medio) y otros terceros curiosos que podrían estar haciéndolo por motivos más que cuestionables y que no tienen ningún derecho a acceder a nuestros datos sensibles. En Estados Unidos, obtener actualizaciones en tiempo real de la ubicación de cualquier móvil cuesta en torno a 12,95 dólares (unos 11 euros). [63] En ese país, este mercado clandestino de datos de ubicación solo se ha confirmado en los casos de T-Mobile, Sprint y AT&T, pero es muy posible que también estén en él otras telecos y que esté funcionando asimismo en otras zonas del mundo.

Todos estos actores —empresas automovilísticas, brókeres de datos, telecos, tiendas y gigantes tecnológicos— quieren saber dónde estás. Puede que te tranquilices convenciéndote de que, aunque es cierto que la cantidad de datos que de ti se recopilan es enorme, gran parte de ellos se anonimizarán. Por desgracia, es muy habitual que los datos anonimizados sean fáciles de reidentificar. Una de las primeras lecciones sobre reidentificación nos la dio el caso de Latanya Sweeney en 1996, cuando la Comisión del Seguro Colectivo de Massachusetts publicó datos anonimizados en los que se mostraban las visitas médicas a hospitales efectuadas por los empleados del estado. El entonces gobernador William Weld tranquilizó a los pacientes asegurando que su privacidad estaba protegida. Sweeney desmintió esas palabras cuando descubrió

su historial médico entre los datos y lo envió por correo a la mismísima jefatura del Gobierno estatal. Posteriormente demostró que se podía identificar al 87 por ciento de los estadounidenses a partir de solo tres datos: su fecha de nacimiento, su género y el código postal de su domicilio. [64]

Otra manera en que se te podría identificar es a través de tu ubicación. Cada persona deja un rastro de ubicaciones diferente, por lo que, incluso si tu nombre no aparece en la base de datos, es fácil averiguar quién eres. La especificidad de los datos de ubicación no es ninguna sorpresa, pues normalmente solo una persona vive y trabaja exactamente donde tú lo haces. Yves-Alexandre de Montjoye, director del Grupo sobre Privacidad Informática en el Imperial College de Londres, estudió quince meses de datos de ubicación de un millón y medio de individuos. De Montjoye y sus colaboradores averiguaron que, en un conjunto de datos en el que se hayan ido registrando las ubicaciones de las personas con una frecuencia horaria y una resolución espacial equivalente a la que proporcionan los teléfonos móviles cuando se conectan a las torres de telefonía, bastan solo cuatro puntos de datos espaciotemporales para identificar de forma exclusiva a un 95 por ciento de los individuos. [65] Él mismo dirigió otro equipo de investigadores que examinó tres meses de registros de tarjetas de crédito de más de un millón de personas y descubrió que no se necesitaban más de cuatro puntos de datos espaciotemporales para reidentificar de manera específica y singular a un 90 por ciento de los individuos. [66]

Muchas veces, las bases de datos pueden desanonimizarse buscando correspondencias con información que es de dominio público. En 2006, Netflix publicó diez millones de puntuaciones de películas de medio millón de sus clientes como parte de un reto dirigido a diseñar un mejor algoritmo de recomendaciones. Se suponía que los datos eran anónimos, pero unos investigadores de la Universidad de Texas en Austin demostraron que podían reidentificar a esas personas comparando sus puntuaciones y marcas temporales con la información pública disponible en la Internet Movie Database (IMDb). Dicho de otro modo, si viste una película una noche determinada, le diste una puntuación positiva en Netflix y luego la calificaste también en la IMDb, estos investigadores podían inferir que fuiste tú quien hizo todo eso. Las preferencias cinematográficas son un material sensible; pueden revelar tendencias políticas y sexuales. Una madre lesbiana demandó a Netflix por el riesgo de revelación no deseada de su orientación sexual que le hizo correr. [67]

Los brókeres de datos inducen a engaño a la población cuando dicen que anonimizan los datos. [68] Comercian con datos personales. Recopilan toda clase de información de extrema sensibilidad, la empaquetan y se la venden a bancos, aseguradoras, comercios, telecos, empresas de medios, administraciones

y, en ocasiones, también a delincuentes. [69] Venden información sobre cuánto dinero ganan las personas, o sobre si están embarazadas o divorciadas o tratan de perder peso. Se sabe asimismo que han vendido listas de víctimas de violación, de pacientes de sida y de otras categorías problemáticas. [70]

También los anuncios en línea usan categorías cuestionables. El Interactive Advertising Bureau, una organización patronal que establece normas para ese sector, emplea categorías para los anuncios dirigidos entre las que se incluye el haber recibido (o estar recibiendo) apoyo contra el incesto o los abusos, o la drogadicción, o el sida y el VIH. También entre los criterios con los que Google selecciona a las personas para su publicidad dirigida están el abuso de sustancias, las enfermedades de transmisión sexual, la impotencia masculina y las inclinaciones políticas. [71] Estas categorías ponen de manifiesto qué les interesa a los buitres de datos: anhelan saber dónde nos duele. Como los depredadores, pueden oler la sangre. Buscan nuestros puntos débiles para explotarlos.

Regresemos a tu día. Te dejamos haciendo la maleta para tu viaje de trabajo a Estados Unidos. Cuando llegas al aeropuerto de Heathrow, es posible que no te pidan la tarjeta de embarque ni al pasar por el control de seguridad, ni al subir al avión. Se está utilizando el reconocimiento facial para verificar la identidad. [72] En Estados Unidos, aerolíneas como JetBlue y Delta ya usan esa tecnología. Y Donald Trump emitió un decreto presidencial que ordenaba la aplicación de la identificación por reconocimiento facial al «cien por cien de los pasajeros internacionales», ciudadanos estadounidenses incluidos, en los veinte principales aeropuertos de Estados Unidos para este año de 2021 (pese a que parecen existir dudas sobre la legalidad de tal medida). [73]

Sigamos con tu viaje. Cuando llegas a tu destino, un funcionario de la Administración para la Seguridad en el Transporte (TSA) te pide que le entregues tu portátil y tu teléfono inteligente. Te muestras reticente, pero entonces él te informa de que, si te niegas a obedecer, se te denegará la entrada en el país. Tienes una reunión de trabajo a la que no puedes faltar. Si tu jefe se entera de que no asististe a ella porque te deportaron por desobedecer a un funcionario en el control de fronteras, no va a estar muy contento. Te preguntas incluso si no podría llegar a despedirte. La perspectiva de quedarte en el paro te empuja a dejar que revisen tu información más privada. Intentas acordarte de qué tipo de datos llevas ahí guardados. Te vienen a la cabeza alguna fotografía desnuda con tu pareja, o las fotos de tus hijos, o toda tu información bancaria.

Entonces recuerdas que ahí también hay información muy privada relacionada con tu empresa. Tal vez tengas secretos comerciales que valen millones. ¿Cómo puedes estar segura de que esos datos no acabarán en manos de un competidor

estadounidense? También puede que tengas información confidencial sobre tu Gobierno que tú misma elaboraste o que adquiriste cuando trabajaste de consultora para este. En 2017, un ingeniero de la NASA fue obligado a desbloquear su teléfono inteligente en la frontera, pese a que llevaba en él contenido muy sensible. [74] Podrías ser una médica que tuviera guardada en su portátil información delicada sobre sus pacientes, o una abogada que quisiera velar por sus clientes, o una periodista interesada en proteger a sus fuentes.

Le dices al funcionario de la TSA que tienes que proteger la información confidencial que llevas, que es tu deber profesional y que podrías sufrir consecuencias judiciales si no lo haces. Nada de eso conmueve en lo más mínimo al agente. Recuerdas haber leído algo en la prensa sobre que, si te deportan de un país, no puedes volver a entrar en él en los cinco o diez años siguientes. Eso sería catastrófico para tu trabajo. Tampoco estás segura de si una «entrada denegada» equivale a una deportación. Pides un abogado. El funcionario de la TSA te responde diciéndote que solo los delincuentes piden un abogado. Te pregunta si tienes algo que ocultar. Cansada e intimidada, terminas cediendo y le entregas el portátil y el teléfono. El agente se lleva tus dispositivos electrónicos a otra estancia, fuera de tu vista, y no regresa hasta un cuarto de hora después. Durante ese rato, el agente se descarga tus datos. [75]

Las fronteras inteligentes se están convirtiendo en amenazas para los derechos civiles; se están desplegando sin haber evaluado antes de forma seria ni sus ventajas, ni sus riesgos, ni sus implicaciones legales y éticas. [76] Drones, sensores y reconocimiento facial son algunas de las tecnologías invasivas que prometen un control de fronteras más barato y eficaz a costa de nuestra privacidad. Ante su fracaso en su empeño por lograr financiación para erigir un muro físico en la frontera con México, la administración de Trump construyó uno virtual hecho de vigilancia. No solo se han instalado sensores en la frontera propiamente dicha, sino también en localidades estadounidenses próximas a ella. [77] Otras iniciativas similares se están proponiendo y probando en todo el mundo. Hungría, Letonia y Grecia han puesto en práctica programas piloto de test automatizados de detección de mentiras en cuatro puntos fronterizos. El sistema, llamado iBorderCtrl, pregunta a los viajeros cosas como «¿Qué lleva usted en la maleta?» y luego trata de identificar «biomarcadores de engaño». [78]

Llegas por fin a tu hotel agotada, enfadada y humillada por semejante violación de tu derecho a la privacidad. Decides hacer algo para minimizar futuras intromisiones. Piensas en escribir un correo electrónico a un abogado especialista en inmigración para estar mejor informada sobre tus derechos, pero, de pronto, te invade el temor a que la TSA, la Agencia de Seguridad Nacional

(NSA) o algún otro organismo tenga acceso a ese mensaje, y que este haga saltar sin más las alertas en los aeropuertos. No quieres pasar a ser la típica persona a la que siempre paran en las fronteras e interrogan durante horas. Sientes, pues, demasiado miedo para pedir asesoramiento jurídico. Tal vez bastaría con reducir los datos que tu teléfono y tu portátil recogen de ti. Eso, como mínimo, sería un comienzo.

Podrías empezar intentando determinar qué datos se descargaron de tu teléfono y de tu ordenador en la frontera. Te bajas los datos que Google y Facebook tienen de ti. [79] Horrorizada al ver el nivel de intrusión que allí has descubierto (Google tiene datos tuyos que creías haber borrado), decides que debes cambiar toda tu configuración de privacidad para minimizar la recopilación de datos. Cuando compruebas cómo está esa configuración ahora mismo, te das cuenta de que todas las opciones marcadas por defecto son las peores para tu privacidad. [80] Y, aunque algunas de ellas pueden modificarse, ves que, si no das tu consentimiento para ciertas formas de recopilación de datos, no podrás usar los servicios que te proporcionan gigantes tecnológicos como Facebook y Google. [81] No tienes margen para negociar los términos y las condiciones, que pueden, además, cambiar en cualquier momento sin previo aviso. [82] Eres víctima de un abuso en toda regla. [83]

Caes en la cuenta entonces de que, en muchos sentidos, te están tratando como a una sospechosa de un delito: el nivel de intrusión, toda esa geolocalización, parecida a llevar una tobillera de seguimiento electrónico, y la contundencia con la que se te imponen estas medidas. En cierto sentido, es peor que ser una presunta delincuente. Al menos, si la policía te detiene, te permite guardar silencio y te advierte de que cualquier cosa que digas podrá ser usada en tu contra. Como súbdita de la tecnología, sin embargo, no dispones de ese derecho a permanecer callada, pues los rastreadores recolectan tus datos, aunque no quieras que lo hagan, y no se te recuerda que estos podrán usarse (y se usarán) en perjuicio tuyo. Además, por lo menos si se te juzgara por un procedimiento penal, siempre te asistiría el derecho a no autoincriminarte. En la sociedad de la vigilancia, sin embargo, tus datos se usan contra ti todo el tiempo.

Tu pareja interrumpe ese hilo de pensamientos con una llamada. Se ha enfadado al ver el Echo en pedazos. Las cosas no van demasiado bien entre ambos desde hace un tiempo. Ojalá tuvieras la serenidad necesaria para explicarle con calma lo ocurrido, pero te sientes derrotada por los acontecimientos. Tu silencio no hace sino aumentar el malestar que tu pareja siente y expresa.

—Lo siento —te dice—. Ojalá estuviéramos cara a cara para decírtelo, pero no puedo soportar esta situación un día más. Quiero el divorcio. Hablaremos de

los detalles cuando vuelvas.

Y te cuelga el teléfono.

Estupefacta, abres Spotify en tu portátil para tranquilizarte con algo de música. El primer anuncio que allí aparece es de abogados matrimonialistas. ¿Casualidad? Casi seguro que no. ¿Cómo se han enterado? ¿Y quiénes? Tal vez haya sido porque tu pareja ha realizado búsquedas en línea relacionadas con el divorcio. O quizá hayan grabado y analizado vuestras discusiones de pareja. O tal vez un algoritmo predictivo haya adivinado que un divorcio estaba al caer en vista del poco tiempo que has pasado últimamente con tu familia. Puede que fuera Spotify la que analizara tu estado de ánimo a partir de tus elecciones musicales. Hasta los bancos miden ahora tu estado de ánimo examinando datos de Spotify. [84] Te molesta la idea de que probablemente nunca llegues a enterarte de quiénes saben que te vas a divorciar, cómo obtuvieron esa información o si lo supieron antes incluso que tú. Sea como fuere, no está bien. Tú no les habías dicho nada y ellos no tenían derecho a espiar tus relaciones más íntimas.

Te preguntas entonces hasta dónde pueden llegar las invasiones de la privacidad antes de que nos decidamos a ponerles freno. La tecnología siempre ha desafiado los límites de la privacidad. Primero fue la fotografía, ahora es internet. Te entra un escalofrío al acordarte de haber leído que Nike ha empezado a vender sus primeras zapatillas inteligentes. [85] Si los investigadores logran desarrollar el llamado «polvo inteligente» (unos sensores ubicuos que no precisan de pilas y son lo bastante diminutos como para resultar casi invisibles), [86] la protección de la privacidad podría ser una misión casi imposible.

Te consuelas pensando que igual, cuando llegue el momento, estarás encantada de irte al otro barrio y abandonar por fin este nuevo mundo feliz. Te apena, eso sí, la idea de que tu hijo haya tenido que lidiar con estos problemas de privacidad desde muy pequeño y de que tenga que seguir peleando con ellos durante mucho más tiempo que tú. Al reflexionar sobre la mortalidad, reparas en que las violaciones de tu derecho a la privacidad no se detendrán ni siquiera cuando te mueras. Tú seguirás viviendo en línea. Los carroñeros continuarán alimentándose del rastro de datos que dejes tras de ti. Y tal vez esa información pueda afectar todavía a tu hijo y a los descendientes que este tenga. También podría influir en la percepción que de tu vida puedan tener otros; tu reputación *post mortem* .

Te preguntas si hay algo que puedas hacer para limpiar tu rastro de datos antes de que sea demasiado tarde. Lo hay. Antes de sucumbir a la desesperanza ante esa pérdida de privacidad a raudales que sufrimos cada segundo del día, continúa leyendo. Los tres capítulos siguientes no dibujan un panorama muy halagüeño,

pero esta disección de las espeluznantes entrañas de la economía de los datos es importante porque nos permite comprender mejor cómo hemos llegado hasta aquí y cómo podemos salir de este lío tan opresivo.

2

¿Cómo hemos llegado a esto?

El contraste entre el paisaje actual de la privacidad y el de la década de 1990 es muy marcado. A finales del siglo XX , tu coche no era más que un coche; no le interesaba saber qué música te gusta, no escuchaba tus conversaciones, no hacía un seguimiento de tu peso, no grababa tus idas y venidas. El coche te llevaba adonde querías ir. Estaba a tu servicio, no al revés. Para algunos, abrir los ojos a esta vigilancia característica de la era digital fue como si nos hubiéramos acostado una noche y nos hubiéramos encontrado con un mundo completamente distinto a la mañana siguiente; un mundo más desolador, al menos en cuanto a nuestra privacidad y a nuestra autonomía con respecto a los objetos que nos rodean. ¿Cómo hemos llegado a esto? ¿Por qué permitimos que arraigara la sociedad de la vigilancia? Por lo menos tres elementos jugaron un papel en la erosión de nuestra privacidad: el descubrimiento de la alta rentabilidad que se podía obtener de los datos personales resultantes de nuestras vidas digitales, los atentados terroristas del 11 de septiembre de 2001 y la errónea creencia de que la privacidad es un valor obsoleto.

CONVERTIR LOS DATOS DE ESCAPE EN POLVO DE ORO

¿Cómo terminan las experiencias de tu vida cotidiana convertidas en datos? Mediante tu interacción con los ordenadores. La informática genera un subproducto en forma de datos. Cuando usas tecnologías digitales —o cuando las tecnologías digitales te usan a ti—, se produce un rastro de datos de lo que has hecho, cuándo y dónde. Al principio de la era digital, esos datos no tenían un uso comercial: o bien no se utilizaban para nada, o bien solo servían de realimentación con la que mejorar el sistema para los usuarios. El protagonista de la historia de la transformación de esos datos de escape en polvo de oro es Google. [1]

Larry Page y Sergey Brin se conocieron cuando estudiaban en la Universidad de Stanford en 1995. En 1996, desarrollaron el núcleo central de Google, el algoritmo PageRank. [2] Este cuenta el número y la calidad de los enlaces a una página para valorar su grado de autoridad y ordena los resultados de una búsqueda en función de esas valoraciones. El algoritmo presupone que los sitios

web más importantes son aquellos con los que otros sitios web de autoridad tienen establecidos más enlaces. Otros motores de búsqueda generaban listados irrelevantes porque se centraban en exclusiva en el texto del contenido de los sitios, sin ponderar los diferentes tipos de fuentes. El algoritmo de Page y Brin, por el contrario, podía dar mayor visibilidad a un periódico de prestigio que a un blog desconocido, por ejemplo.

PageRank se inspiraba en el modelo de las citaciones académicas. Los académicos escriben artículos basados en parte en trabajos previos de otras personas que citan. Cuantas más citas obtiene un artículo en otros textos, mayor es la importancia que se le atribuye. Imitando esta práctica del mundo académico, PageRank logró imponer un orden en medio del ruido carente de sentido que era internet y, de ese modo, hizo que las búsquedas fueran mucho más informativas y valiosas. Fue una idea brillante. Y no quedó ahí la cosa: el algoritmo fue mejorando progresivamente a medida que crecía internet. Demostró una escalabilidad espectacular. [3]

Por desgracia para todos nosotros, el problema vino cuando Page y Brin se propusieron transformar el buscador de Google para que pasara de ser una asombrosa herramienta a convertirse en un negocio muy lucrativo. A comienzos de 1999, trataron de vender Google a Excite, la empresa de otro motor de búsqueda, pero la operación se frustró. Se dice que también intentaron venderlo a AltaVista y a Yahoo. [4] En 2000, dos años después de haberse constituido como sociedad empresarial y pese a que su popularidad iba en aumento, Google seguía sin haber desarrollado un modelo de negocio sostenible. Podría decirse que aún era una más de las típicas *startups* de internet que no generaban beneficios. Los inversores se impacientaban. Uno de ellos bromeó diciendo que lo único que había recibido por su inversión de seis cifras era «la camiseta más cara del mundo». [5] La empresa corría el riesgo de que quienes la financiaban se retiraran del proyecto si no empezaba a ganar dinero. La situación económica de Google era desesperada.

Esta no tardaría en dar un vuelco. En 2001, los ingresos de Google se incrementaron hasta los 86 millones de dólares (habían sido de 19 millones en el año 2000). En 2002, esa cifra se disparó hasta los 440 millones, y luego hasta los 1.500 millones en 2003, y hasta los 3.200 millones en 2004. Hablamos, pues, de un incremento de los ingresos del 3.590 por ciento en solo cuatro años, de 2001 al final de 2004. [6] ¿Cómo lo lograron? No, no atracaron ningún banco ni descubrieron petróleo bajo sus pies, o no exactamente. Usaron los datos personales de sus usuarios para vender anuncios e inauguraron así la era del «capitalismo de la vigilancia», como la psicóloga social Shoshana Zubofftan brillantemente la ha bautizado.

Antes de convertirse en los grandes maestros mundiales de los anuncios, los dueños de Google no tenían una impresión demasiado favorable de la publicidad. Al menos, eso decían ellos. Brin y Page escribieron un artículo en 1998 en el que manifestaban la preocupación que les producía la idea de tener que depender de los anuncios. «Nuestra previsión es que los motores de búsqueda financiados con publicidad mostrarán un sesgo inherente favorable a los anunciantes y adverso a las necesidades de los consumidores», vaticinaban. En ese artículo daban a entender que querían que Google conservara su carácter de herramienta académica: «Creemos que el problema de la publicidad da pie a suficientes incentivos mixtos como para que resulte crucial disponer de un motor de búsqueda competitivo que sea transparente y se mantenga en el ámbito de lo académico». [7] Es una lástima que las cosas cambiaran tanto. PageRank era más fiable que otros motores de búsqueda precisamente porque no dependía de la publicidad para ser rentable y, por lo tanto, no necesitaba sesgar sus resultados. A juzgar en exclusiva por aquel artículo, Brin y Page no parecían ser candidatos a convertirse algún día en los artífices de la transformación de internet en un mercado publicitario.

Eric Veach fue la persona que diseñó la ingeniería del sistema de anuncios que hizo de Google lo que es hoy. «Detesto los anuncios», dijo en una ocasión, haciéndose eco de la postura de Brin y de Page. [8] En favor de los pioneros de Google cabe alegar que, según parece, su pretensión inicial era hacer anuncios mejores que los típicos de la publicidad en línea en aquel entonces. La teoría de AdWords —como llamaron a aquel sistema— suena bastante razonable: los anuncios debían hacer felices a Google, a los anunciantes y a los usuarios. Google ganaría dinero, los anunciantes lograrían publicitar y vender sus productos, y los usuarios conseguirían a cambio un motor de búsqueda de alta calidad y verían solo la publicidad que pudiera interesarles. No parecía un mal trato.

Una particularidad de AdWords era que los anunciantes no compraban directamente las mejores posiciones en las páginas de resultados. Los anuncios que lograban que más usuarios hicieran clic en ellos se priorizaban; de ese modo, se garantizaba que la publicidad destacada fuese aquella que resultara más útil para los usuarios. No obstante, el sistema era fácil de trampear: los anunciantes podían hacer clic en sus propios anuncios para ganar visibilidad. De ahí que Google decidiera sustituir el sistema original por otro de subastas de anuncios. A partir de entonces, los anunciantes pagarían por clic; es decir, presentarían ofertas de lo que estaban dispuestos a pagar por cada vez que un usuario hiciera clic en su anuncio. El anunciante cuya puja fuera la ganadora quedaría obligado a pagar por clic la cantidad de la segunda puja más alta más un céntimo. Este

inteligente sistema supuso toda una revolución. Al cobrar por clic, Google hizo que los anunciantes pagaran los anuncios solo cuando estos funcionaban. Otra innovación de Google fue la introducción de una reducción de precio para aquellos anuncios que se demostrasen más efectivos, lo que mejoró la calidad de su publicidad.

Los anuncios de Google, en comparación con otros, tenían muchos méritos. Eran relativamente discretos, llevaban bien indicado el aviso «patrocinado» y no se entremezclaban con las búsquedas «orgánicas» del usuario; además, la empresa ofrecía incentivos para potenciar la calidad de esa publicidad. Sin embargo, el sistema también presentaba otros aspectos no tan aceptables. Uno era que representaba una especie de «caja negra» para los anunciantes, que tenían que confiar en los cálculos de Google y nunca llegaban a conocer del todo cómo la tecnológica posicionaba sus anuncios ni por qué. [9] Un inconveniente aún mayor del nuevo régimen de anuncios de Google fue que invirtió por completo el modelo de negocio de la compañía. Los usuarios de Google dejaron de ser los clientes de la empresa, que pasaron a ser los anunciantes. Y nosotros, los usuarios, nos convertimos en el producto. Los incentivos y las lealtades de Google dieron un giro radical.

Desde entonces, Google ha sido y es una empresa de publicidad. Ganó casi 135.000 millones de dólares en 2019 solo con anuncios. Alphabet, propietario de Google, registró unos ingresos totales de casi 162.000 millones de dólares ese año. Dicho de otro modo, más del 80 por ciento de las ganancias de Alphabet proviene de los anuncios de Google. [10] Y AdWords sigue siendo la más rentable de las iniciativas publicitarias de Google. [11]

Como ya te habrás imaginado, la víctima más problemática del éxito de los anuncios de Google fue nuestra privacidad. Nuestros datos, que hasta entonces solo se habían usado para mejorar el motor de búsqueda de la compañía, comenzaron a utilizarse para personalizar mensajes publicitarios. Mediante nuestras búsquedas, Google fue construyendo una imagen precisa de nuestras opiniones y maneras de pensar, tanto colectivas como individuales.

Tendemos a realizar búsquedas relacionadas con lo que estamos pensando en cada momento. El 28 de febrero de 2001, se produjo un terremoto cerca de Seattle a las 10.54 horas de la mañana. Google ya lo había identificado a las 10.56 tras haber detectado en aquella zona una subida repentina en el número de búsquedas relativas a seísmos. [12] También sabe qué programas de televisión son los más populares en cada momento. Y tiene acceso a más información privada todavía, como, por ejemplo, si te estás planteando consumir drogas o abortar, o si te preocupa tu salud o no poder afrontar los pagos de un préstamo. Una muestra en vivo de todas esas búsquedas se exponía en Google mediante

una visualización llamada Live Query. Una periodista de *The New York Times* escribió que mirar Live Query era como «ver pasar ante ti la conciencia colectiva del mundo». [13]

Todos esos datos pueden utilizarse para vender anuncios. En 2003, la idea ya estaba bastante bien desarrollada y los informáticos de Google presentaron una solicitud de patente llamada «Generación de información de usuario para su uso en publicidad dirigida». [14] Las patentes son una buena manera de saber qué andan tramando las compañías. Esta no solo describía cómo dirigir anuncios a usuarios concretos a partir de los datos que estos dejaban tras de sí en sus búsquedas en Google, sino que también explicaba cómo inferir datos que los usuarios podrían no haber facilitado de forma «voluntaria». Lo que aquella patente mostraba, entre otras cosas, era que Google había pasado de recibir datos generados por los usuarios al interactuar con su sitio web (y de utilizarlos para mejorar su servicio) a *crear* y *cazar* datos de los usuarios con la finalidad expresa de emplearlos para dirigir mejor los anuncios.

Mientras los usuarios realizaban búsquedas sobre lo que les apetecía, o sobre lo que les daba miedo, o sobre lo que les producía curiosidad, Google recopilaba montañas de datos sobre ellos. El problema para la compañía era que, en cuanto esos usuarios hacían clic en uno de los resultados de la búsqueda y entraban en otro sitio web, pasaban a estar fuera del alcance de Google. Sin embargo, eso solo fue hasta que el gigante tecnológico diseñó AdSense para complementar su AdWords. AdSense utiliza internet como si fuera un lienzo en blanco listo para ser empapelado con sus anuncios; está en casi todas partes en la web. Publica anuncios en sitios web que son (o eran) independientes de Google, como comercios en línea y páginas de periódicos. Con AdWords y AdSense, Google dio el pistoletazo de salida de la economía de la vigilancia.

Antes de Google, se vendían y se compraban algunos datos personales de manera más esporádica. Y una parte de ellos se usaban con fines publicitarios, pero no a una escala tan grande, ni con semejante nivel de especificidad y análisis, ni con la finalidad de personalizar, ni como principal plan de financiación de buena parte de internet. Google logró transformar los datos de escape en polvo de oro e inauguró la economía de la vigilancia —uno de los modelos de negocio más lucrativos de todos los tiempos. Combinó todos los ingredientes existentes, añadió alguno más y horneó la mezcla. Dio inicio así a una especie de carrera hacia el abismo moral, pues otras compañías enseguida trataron de ponerse al día desarrollando sus propias variantes de minería de nuestros datos personales. Google había convertido a sus usuarios en productos, y otros siguieron su ejemplo.

Para prolongar su hegemonía en la economía de la vigilancia, [15] Google

adquirió en 2007 DoubleClick, una empresa de publicidad que utilizaba una *cookie* (un pequeño paquete de datos que identifica a los visitantes de los sitios web) para acceder a los datos personales de los usuarios, incluidos sus historiales de navegación, antes incluso de que hicieran clic en un anuncio. DoubleClick también usaba anuncios de *display* (*banners* gráficos), algo que contravenía la postura inicial de Google al respecto de no crear anuncios que distrajeran al usuario. Gracias a DoubleClick, Google pudo empezar a seguir a los usuarios a casi cualquier lugar al que iban en la red, aunque no hicieran clic en ningún anuncio. [16] Desde entonces, ha creado un producto tras otro para facilitarse la recogida de cada vez más datos de cada vez más fuentes. Chrome, Maps, Pixel, Nest y otros muchos se diseñaron como sistemas con los que reunir aún más datos de todos nosotros. ¿Por qué iba una empresa a ofrecer un servicio añadido como Maps, algo que tanto esfuerzo cuesta crear y mantener, si no obtuviera nada a cambio? No lo haría. Lo que Google quería era extraer nuestros datos de ubicación.

La mayoría nos enteramos de las cuestionables prácticas que nuestros presuntos héroes tecnológicos estaban llevando a cabo en la trastienda cuando ya era demasiado tarde. Google y otras empresas empezaron a rentabilizar la recopilación, el análisis y el comercio de nuestros datos personales sin pedir permiso a los gobiernos, ni solicitar a los usuarios su consentimiento. Simplemente siguieron adelante con sus planes guiados por la máxima de «a ver qué pasa». Y no pasó nada. Hechizados por los novedosos servicios «gratuitos», los usuarios aceptamos lo que nos parecía un chollo, sin darnos cuenta de a qué estábamos renunciando.

La primera vez que te abriste una cuenta de correo electrónico, probablemente no se te pasó por la cabeza que estabas cediendo tus datos personales a cambio. Desde luego, a mí no se me ocurrió. Sin embargo, el trato no fue ni justo ni claro. Lo de que los usuarios entregábamos de manera consciente nuestros datos a cambio de unos servicios fue un relato que se nos contó años después de que el trato inicial se hubiera sellado, cuando las tecnológicas tenían ya nuestros datos y a nosotros nos parecía impracticable renunciar a esa transacción.

Nunca resultó más evidente que nuestra interacción con las tecnologías digitales no es del todo voluntaria que durante los meses del confinamiento debido al coronavirus. La gente tuvo que usar entonces —para su trabajo, para no interrumpir la escolarización de sus hijos, o para mantenerse en contacto con la familia— tecnologías que son muy poco respetuosas con la privacidad. Desde el momento en que las plataformas digitales se convirtieron en indispensables, en obligatorias para poder participar de lleno en nuestra sociedad, ya no hubo posibilidad de autoexcluirnos de forma voluntaria de la recopilación de datos.

No te confundas: no es casualidad que te enteraras de la existencia del capitalismo de la vigilancia mucho después de que se hubiera vuelto prevalente. Google guardó un especial silencio sobre sus iniciativas de recolección de datos personales y su modelo de negocio. [17] El entonces director ejecutivo de la compañía, Eric Schmidt, lo llamó «la estrategia de la ocultación». [18] El secretismo fue un modo de proteger su ventaja competitiva durante el máximo tiempo posible. Fue también una manera de mantener a los usuarios en la ignorancia a propósito de lo que se hacía con sus datos. Douglas Edwards, un antiguo ejecutivo de Google, escribió en ese sentido que «Larry [Page] se oponía a que siguiéramos cualquier camino que revelara nuestros secretos tecnológicos o que agitara el avispero de la privacidad y pusiera en peligro nuestra capacidad de reunir datos. La gente no sabía cuántos recopilábamos, pero no estábamos haciendo nada malo con ellos, así que ¿por qué iniciar un debate que solo serviría para confundir y preocupar a todo el mundo?». [19] Como veremos, sí que debería preocuparnos que nuestros datos privados se recolecten, aunque nadie los esté usando en ese momento con fines perniciosos: lo normal es que, tarde o temprano, alguien termine por hacer un uso indebido de ellos. Además, la maldad de un uso no siempre es evidente de entrada, sobre todo cuando forma parte de un sistema. La economía de los datos ha llevado, años después, a la erosión de la igualdad y la democracia. Por eso, el derecho a la privacidad es justo eso, un *derecho* , y debemos respetarlo incluso cuando los efectos negativos no nos resulten obvios de inmediato.

Google mantuvo la boca cerrada con respecto a su modelo de negocio porque se estaba llevando algo muy privado de nosotros sin pedirnos permiso y lo estaba usando en provecho de sus anunciantes y en el suyo propio. [20] Y nadie detuvo a Google porque casi nadie sabía lo que sucedía. Sin embargo, las cosas podrían haber sido distintas. La economía de la vigilancia no era inevitable. Brin y Page podrían haber obtenido sus plazas de profesores universitarios y haber hecho que el buscador de Google siguiera siendo una especie de iniciativa académica no comercial, algo así como Wikipedia. O podrían haber encontrado un modelo de negocio alternativo. O podrían haber sido los organismos reguladores los que hubieran intervenido limitando lo que se podía hacer con nuestros datos privados. De hecho, hubo un tiempo en que casi se llegó a regular la economía de los datos, pero una catástrofe se interpuso en el camino.

Y ENTONCES LLEGÓ EL DESASTRE

A finales de la década de 1990, las *cookies* ya habían empezado a preocupar a

los organismos reguladores. En 1996 y 1997, en dos jornadas de la Comisión Federal de Comercio (FTC) de Estados Unidos, se habló de dejar en manos de las propias personas el control sobre su información personal. El enfoque inicial de la FTC fue animar a las empresas a autorregularse en ese sentido. Sin embargo, estas no hicieron caso. En 1999, por ejemplo, DoubleClick se había fusionado con un bróker de datos, Abacus, con la presumible intención de tratar de identificar a sus usuarios. Varias organizaciones de defensa de la privacidad solicitaron a la FTC que investigara la operación y esta presionó a DoubleClick para que vendiera Abacus. [21]

Cuando se hizo evidente que la autorregulación no bastaría para proteger la privacidad de los usuarios, la FTC dio un paso más. En 2000 redactó un informe dirigido al Congreso con una propuesta legislativa. En él sugería que se obligara a los sitios web a informar a los usuarios sobre sus prácticas de uso de la información, a permitir que los usuarios eligieran cómo se utilizarían sus datos, a permitir también que los individuos accedieran a los datos personales que los propios sitios web tuvieran sobre ellos y a proteger la seguridad de la información que recopilasen. «La Comisión entiende que el éxito limitado con el que el sector ha implantado buenas prácticas en cuanto a la gestión de la información en línea, unido a las crecientes preocupaciones de los consumidores sobre la privacidad de internet, hacen que este sea el momento apropiado para tomar medidas legislativas», se podía leer en el informe. [22] Si Estados Unidos hubiera aprobado entonces legislación encaminada a frenar la recolección en línea de datos personales, tal vez nuestro mundo sería muy diferente en la actualidad. Es posible que Google no se hubiera convertido en un gigante publicitario y que las prácticas de la vigilancia que tan extendidas están hoy nunca hubieran llegado a desarrollarse.

Lamentablemente, sin embargo, la historia siguió un curso muy distinto. Poco más de un año después de la publicación de ese informe de la FTC, en septiembre de 2001, unos terroristas secuestraron cuatro aviones de pasajeros en Estados Unidos. Dos impactaron contra las Torres Gemelas en Nueva York, otro contra el Pentágono y el cuarto —que, al parecer, se dirigía hacia la Casa Blanca — se estrelló en Pensilvania después de que sus pasajeros se enfrentaran a los secuestradores. Aquel ataque no solo se cobró la vida de casi tres mil personas, sino que desencadenó una guerra, se utilizó para justificar la aprobación de medidas legislativas extraordinarias e infligió un trauma nacional e internacional cuyos efectos aún perduran. Por desgracia, aquellos atentados terroristas fueron muy efectivos en su propósito de herir la democracia liberal. Y parte del daño lo causaron los propios representantes democráticos.

Tras el 11-S, la consigna, anunciada por el presidente George W. Bush y

secundada por la sociedad estadounidense durante años, fue: «Nunca más». Imperaba cierto sentimiento de vergüenza por no haber prevenido los atentados y la determinación de hacer lo que fuera necesario con tal de que jamás volviera a producirse un nuevo 11-S. De la noche a la mañana, el eje central de la acción gubernamental en Estados Unidos pasó a ser la seguridad. Se aparcó la cuestión de la regulación de los datos. [23] Y no fue solo porque el Gobierno estuviera demasiado ocupado impulsando la seguridad y no tuviera tiempo para abordar la privacidad. Las agencias de inteligencia vieron ante sí la oportunidad de ampliar sus poderes de vigilancia obteniendo una copia de todos los datos personales que las empresas privadas estaban recopilando. [24] Desde el momento en que el Estado comenzó a interesarse por nuestros datos personales, dejó de tener aliciente alguno para regular la protección de la privacidad. Al contrario: cuantos más datos recolectaran las empresas, más potente podría ser la vigilancia gubernamental y más atentados terroristas podrían prevenirse... en teoría.

El Congreso federal aprobó la Ley Patriota, instauró un programa de cribado terrorista y promovió toda una serie de medidas que incrementaron el margen para la vigilancia sin orden judicial. Muchas de las iniciativas emprendidas fueron encubiertas: leyes secretas, tribunales secretos, políticas secretas. Una década después del 11-S, un ciudadano corriente no podía saber cuál era el estado real de la vigilancia y de los derechos civiles en Estados Unidos porque no se había revelado aún la totalidad de las normas que regulaban la sociedad estadounidense. [25] En realidad, la mayor parte de lo que hoy sabemos sobre vigilancia masiva en Estados Unidos lo descubrimos gracias a las revelaciones de Edward Snowden, un empleado de una consultoría privada contratada por la Agencia de Seguridad Nacional (NSA) que, en 2013, se convirtió en denunciante clandestino de las prácticas de esta. [26]

El alcance de los poderes de vigilancia que ha acumulado el Gobierno en Estados Unidos tras el 11-S es extraordinario. Para entrar en detalles sobre el tema, haría falta un libro entero, [27] pero he aquí una pequeña degustación. La NSA recopiló datos de Microsoft, Yahoo, Google, Facebook, YouTube, Skype y Apple, entre otras compañías, a través de un programa denominado PRISM. Entre el contenido recogido figuraban correos electrónicos, fotografías, conversaciones en vídeo y audio, historiales de navegación y todos los datos almacenados en sus nubes. Y, por si eso fuera poco, la NSA también llevó a cabo una recopilación *upstream* de datos, es decir, recogiéndolos directamente de elementos infraestructurales de internet del sector privado, desde enrutadores hasta cables de fibra óptica. [28]

La NSA utilizó entonces XKEYSCORE para organizar todos los datos que había reunido. XKEYSCORE era una especie de buscador que permitía que los

analistas, con solo teclear el domicilio, el teléfono o la dirección IP de cualquier individuo, pudieran estudiar su actividad reciente en línea. Allí estaban las comunicaciones de todo el mundo. Los analistas también podían observar la actividad de las personas en vivo y lo que estaban tecleando, letra por letra, en cuanto estas entraban en algún entorno conectado en línea. [29]

La mayor parte del tráfico mundial de internet pasa por infraestructuras o tecnologías que están bajo el control de Estados Unidos. [30] Eso significa que la NSA puede vigilar a casi todos los usuarios de internet del mundo. Y, si da la casualidad de que eres una persona de interés para la NSA, su vigilancia puede hacerse más intrusiva aún, pues la agencia dispone de programas capaces de acceder a todos los rincones de tu vida digital y de manipularla. [31] Si le resulta útil para sus propósitos, la NSA puede compartir con otras agencias de inteligencia de países aliados algunos de los datos que ha recopilado. La NSA quiere reunir y mantener un registro permanente de todo. [32] En los servicios de inteligencia denominan a tal invasión de la privacidad «recogida de datos al por mayor» para no llamarla por su verdadero nombre: *vigilancia masiva* .

Lo más triste de nuestra pérdida de privacidad es que ni siquiera sirvió para prevenir el terrorismo. La idea de que, si disponemos de más datos sobre las personas, podremos impedir que sucedan cosas malas como atentados terroristas es bastante intuitiva. Su atractivo resulta comprensible. Sin embargo, es un error. Toda la evidencia de la que disponemos indica que la vigilancia masiva en Estados Unidos ha sido absolutamente inútil para prevenir el terrorismo. El Grupo Presidencial de Evaluación de las Tecnologías de Inteligencia y Comunicaciones, por ejemplo, no logró hallar un solo caso en el que la recopilación masiva de registros de llamadas telefónicas hubiera impedido un atentado. [33]

En 2004, el FBI analizó la información de inteligencia reunida gracias a STELLARWIND, un programa de vigilancia que aunaba una serie de actividades de recogida al por mayor de datos de comunicaciones telefónicas y por correo electrónico, para comprobar cuántas de esas actividades habían realizado alguna «contribución significativa» a la identificación de terroristas, la deportación de sospechosos o la conexión con algún informante que aportara detalles sobre esa clase de grupos o individuos. Solo un 1,2 por ciento de las pistas obtenidas por esa vía entre 2001 y 2004 fueron útiles. Cuando el FBI examinó los datos de 2004 a 2006, descubrió que ninguna de las pistas de ese periodo había producido una contribución significativa. [34] Los indicios remitidos por la NSA al FBI demostraron ser un verdadero derroche, tanto por su desproporcionado volumen como por el tiempo que se perdió en darles seguimiento. [35] Cuando la NSA se quejó al FBI por los escasos resultados que

este estaba sacando de la información que aquella le estaba transfiriendo, un alto funcionario del buró respondió trasladando a la agencia la respuesta que había recibido de sus subordinados: «Nos estáis enviando basura». [36]

El terrorismo es una actividad infrecuente; tratar de anticiparse a él es como buscar una aguja en un pajar. Arrojar más paja al montón no facilita de ningún modo esa búsqueda, sino que más bien la dificulta. Al recopilar muchos más datos irrelevantes que relevantes, la vigilancia masiva añade más ruido que señal. [37] Y aun si esta clase de vigilancia pudiera impedir atentados, debemos tener presente que no está exenta de riesgos y daños. El peligro de que se produzca un atentado terrorista debe sopesarse con el riesgo de que se haga un mal uso masivo de los datos, y con una consiguiente erosión de los derechos civiles. Como veremos, las pérdidas de privacidad también matan.

En las dos décadas de su existencia, la vigilancia masiva no parece haber evitado el terrorismo, pero sí ha sido muy eficaz despojando a todos los usuarios de internet de su derecho a la privacidad. La vigilancia se ha usado asimismo con fines de espionaje económico e internacional; sus objetivos han incluido a países aliados y a organismos de cooperación. [38] La principal aportación de la vigilancia digital masiva ha consistido, pues, en dar más poder a los poderosos —tanto a las empresas de tecnología que pronto se convirtieron en las «grandes tecnológicas» como a los gobiernos— y en quitárselo al ciudadano de a pie.

Son varias las lecciones que podemos extraer de este deprimente episodio de nuestra historia. Una de ellas nos la enseña el hecho de que la sociedad de la vigilancia nació de la colaboración entre instituciones privadas y públicas. El Estado permitió que la recopilación de datos realizada por empresas privadas prosperara para poder hacerse una copia de la información. Los gobiernos permitieron que la economía de los datos creciera descontrolada porque esta demostró ser una buena fuente de poder para ellos. A cambio, las compañías pusieron de su parte colaborando en la vigilancia estatal. AT&T, por ejemplo, instaló equipos de vigilancia a petición de la NSA en al menos diecisiete de sus núcleos de distribución de internet en Estados Unidos. También proporcionó ayuda técnica para intervenir todas las comunicaciones por internet en la sede central de las Naciones Unidas, una organización cliente de dicha compañía. [*] [39]

Tal vez el mejor ejemplo de hasta qué punto el capitalismo de la vigilancia es una iniciativa público-privada sea Palantir. Así llamada en honor a las omniscientes bolas de cristal de *El señor de los anillos* , de J. R. R. Tolkien, Palantir es una muy reservada empresa de análisis de macrodatos. La fundó Peter Thiel [**] [40] en 2004 con financiación de la CIA y siguiendo un plan de diseño realizado en colaboración con las agencias de inteligencia. Se especializa

en detectar información relevante entre montañas de datos.

Uno de los problemas de XKEYSCORE, la herramienta de la NSA que funcionaba como un motor de búsqueda, era la sobrecarga de datos. Por ejemplo, buscar entre todas las direcciones IP desde las que se habían efectuado llamadas de Skype en un determinado momento podía producir demasiados resultados. Era como si quisieras efectuar una búsqueda en tu cuenta de correo, pero los resultados que aparecieran fueran de todas las cuentas de correo electrónico de todo el mundo. Palantir ayudó a la NSA a hacer que XKEYSCORE resultara más comprensible. [41]

Esa cooperación público-privada continúa vigente. La mayoría de los países no disponen del conocimiento experto necesario para desarrollar herramientas de vigilancia y jaqueo, así que se las compran a los fabricantes de «ciberarmas». [42] Países de todo el mundo recurren a los gigantes tecnológicos para fines de vigilancia. Palantir, Amazon y Microsoft, por ejemplo, suministraron herramientas que ayudaron a la administración Trump a vigilar, detener y deportar a inmigrantes, [43] medidas excepcionalmente controvertidas todas ellas porque comportaron que muchas niñas y niños pequeños fueran separados de sus padres o madres. [44] Se sabe desde hace tiempo que los centros comerciales de Estados Unidos captan los números de las matrículas de los automóviles e incorporan esas imágenes a unas bases de datos que luego usan los cuerpos y fuerzas de seguridad. Algunas grandes empresas también informan a la policía sobre cómo acceder a los datos que almacenan de sus clientes. En agosto de 2019, varios representantes de AT&T, Verizon, Sprint, T-Mobile y Google acudieron como «conferenciantes» invitados a un seminario, «Capacidades de los operadores de redes móviles y de los proveedores de servicios de internet para los investigadores policiales», en el que se trataron temas como «la interpretación y el uso de datos móviles». [45] En las actas de algunos tribunales estadounidenses constan peticiones de inspectores o fiscales a Google, no ya de información sobre algún sospechoso conocido, sino incluso sobre cualquiera que haya realizado una búsqueda con una determinada palabra clave. [46] Probablemente no sea casualidad que una de las nuevas sedes de Amazon esté tan cerca del Pentágono. A la vista de los estrechos lazos que las unen, no tiene mucho sentido distinguir entre la vigilancia de los estados y la de las empresas privadas. Tenemos que hacer frente a ambas.

Si nos protegemos solamente del Estado, las empresas nos vigilarán y pasarán esa información a los gobiernos. En 2018, John Roberts, presidente del Tribunal Supremo de Estados Unidos, redactó la opinión de la mayoría de este en la sentencia que prohibía al Gobierno obtener datos de ubicación de las torres de telefonía móvil sin una orden judicial previa. Su argumento era que, «cuando el

Gobierno rastrea la ubicación de un móvil, consigue un nivel casi perfecto de vigilancia, similar al que se alcanzaría acoplando una tobillera de seguimiento al usuario de un teléfono». La sentencia arañaba así para los estadounidenses, casi dos décadas después del 11-S, parte de la privacidad perdida. Sin embargo, en el contexto de una economía de la vigilancia ya asentada, poco podía influir, pues son muchas las vías por las que se pueden obtener datos. En vez de pedírselos a las compañías de telefonía móvil, por ejemplo, la administración Trump compró el acceso a una base de datos comercial que sitúa en el mapa los movimientos de millones de teléfonos móviles en Estados Unidos. Como se trata de datos que se compran a brókeres de datos, el Gobierno no necesita una orden judicial para obtenerlos. Externalizando la vigilancia a base de subcontratársela a compañías privadas, el Gobierno estadounidense halló el modo de sortear las sentencias del Tribunal Supremo. [47]

Si solo nos protegemos de la vigilancia de las compañías privadas, el Estado recopilará datos y se los pasará a las empresas. El flujo de información circula en ambos sentidos. En Reino Unido, por ejemplo, se han vendido datos de millones de pacientes del Sistema Nacional de Salud (NHS) a empresas farmacéuticas. [48] Las grandes tecnológicas no perdieron ni un segundo en iniciar conversaciones con gobiernos de todo el mundo sobre cómo atajar la pandemia de coronavirus mediante el uso de aplicaciones para teléfonos inteligentes. Precisamente la pandemia nos conduce a la segunda lección que podemos extraer de lo ocurrido con la vigilancia a partir del 11-S: *las crisis son peligrosas para los derechos civiles* .

Durante las crisis se toman decisiones sin considerar con detenimiento los pros, los contras, las pruebas y las alternativas. Cualquier mínima resistencia que suscite una determinada propuesta de medidas extremas se puede silenciar en esos momentos apelando a la necesidad de «salvar vidas». Nadie quiere interponerse en el camino de las iniciativas dirigidas a evitar muertes, ni siquiera cuando no hay ni la más mínima prueba de que en verdad las eviten. Los organismos públicos y las empresas privadas tratan entonces de conquistar poder. Se sacrifican derechos civiles de forma injustificable y sin que se establezcan unas garantías efectivas de que estos se recuperarán cuando pase la crisis. Las medidas extraordinarias que se adoptan en un clima de pánico tienden a permanecer mucho tiempo después de que la emergencia se haya superado.

La del «nunca más» fue una reacción poco realista a los atentados del 11-S. Se trataba de un eslogan simple y absurdo que distorsionó durante más de una década los debates sobre políticas públicas. [49] La invulnerabilidad es una quimera. Deberíamos desconfiar de cualquier propuesta política que prometa el riesgo cero. El riesgo solo desaparecerá cuando hayamos dejado de respirar y

estemos a dos metros bajo tierra. Vivir es arriesgar, y vivir bien es gestionar ese riesgo sin comprometer aquello que constituye una vida buena. En el mundo suceden cosas terribles, como atentados terroristas o epidemias, y seguirán sucediendo. Pensar que podremos evitar que ocurran si renunciamos a nuestra libertad y a nuestra privacidad es como creer en los cuentos de hadas. Esa confusión de los deseos con la realidad solo puede llevarnos a sumar el autoritarismo a la lista de catástrofes a las que nos tendremos que enfrentar. Irónicamente, el autoritarismo sí es un desastre que podemos evitar. Para ello tenemos que defender nuestros derechos civiles. Y eso significa proteger nuestros datos personales. La paradoja, pues, está en que el exceso de aversión al riesgo puede abocarnos más adelante a peligros mayores.

Es difícil acordarse del valor de la privacidad cuando se está en medio de una situación de emergencia. Cuando tememos por nuestras vidas, en lo último en que pensamos es en nuestros datos personales. Los peligros del terrorismo y de las epidemias son mucho más tangibles que las amenazas a la privacidad. Un atentado terrorista deja al instante un rastro de cadáveres, personas cuya desaparición lamentamos y que, al mismo tiempo, sirven de advertencia para los que seguimos vivos. Una epidemia presenta efectos menos inmediatos —según parece, el coronavirus de 2020 tarda entre una y dos semanas en enviar a una persona al hospital—, pero deja igualmente un rastro de muerte que, como resulta comprensible, puede infundir terror en el ánimo de la población. Sin embargo, las pérdidas de privacidad también pueden ser letales, tanto en un sentido literal como en el —más metafórico— de acarrear la muerte de modos de vida que valoramos; la diferencia es que sus víctimas suelen materializarse mucho más tarde.

La recopilación de datos no nos inflige heridas físicas ni hemorragias; tampoco nos infecta los pulmones ni dificulta nuestra respiración. Aun así, la recolección de datos está intoxicando nuestra vida, nuestras instituciones y nuestras sociedades. La única diferencia es que sus consecuencias tardan un tiempo en desdoblarse. Los datos personales son tóxicos, pero su veneno es de acción lenta.

Será más probable que protejamos nuestros datos personales de un modo adecuado, incluso durante una crisis, si nunca perdemos de vista el porqué de la importancia de la privacidad.

OLVIDAR LO QUE IMPORTA Y POR QUÉ IMPORTA

En 2010, el fundador de Facebook, Mark Zuckerberg, insinuó que la privacidad

había dejado de ser «una norma social» y que la habíamos superado porque habíamos «evolucionado». «La gente no solo se siente ahora muy a gusto compartiendo más información y de diferentes tipos, sino haciéndolo de forma más abierta y con más personas», dijo. [50] No parece que aquellas declaraciones fueran una valoración certera ni sincera de la realidad, a juzgar por las cuatro casas que Zuckerberg se compró alrededor de la suya para disponer de una mayor privacidad. [51] Y tampoco hay que olvidar que la totalidad de los ingresos de Facebook dependen de la explotación de nuestros datos personales. Un mes antes de que Zuckerberg emitiera aquel certificado de defunción de la privacidad, Facebook había introducido un cambio muy controvertido en la configuración por defecto de su plataforma dirigido a obligar a los usuarios a compartir más información en público. [52] A los gigantes tecnológicos les interesa que creamos que la privacidad está pasada de moda, que es un anacronismo. Sin embargo, no lo es.

Un anacronismo es algo que corresponde a un periodo temporal distinto y que suele hacer referencia a cosas que se han vuelto obsoletas. Resulta habitual que heredemos objetos, normas sociales y leyes que se pensaron para un contexto muy diferente y que resultan disfuncionales en la época presente. Algunos anacronismos son graciosos. En Christ Church, mi anterior *college* de la Universidad de Oxford, a la única persona a quien le estaba permitido tener un perro era al «conserje mayor». Para sortear tan desfasada norma, en la década de 1990, el perro del decano tuvo que ser considerado oficialmente un gato. [53] Otro ejemplo: a los parlamentarios del Reino Unido no se les permite llevar armadura en la sede del legislativo nacional. [54] Sin embargo, no todos los anacronismos resultan igual de divertidos, y algunos son muy perjudiciales.

En general, los países tienen muchos miles de leyes y de regulaciones. Es difícil estar al tanto de todas, y no siempre nos acordamos de revocar normas que ya no deberían estar en vigor. Las normas anacrónicas son peligrosas porque pueden usarse con fines cuestionables. Por ejemplo, en 2011, para arrestar a manifestantes del movimiento Occupy Wall Street, se invocó una olvidada ley neoyorquina de 1845 que prohíbe llevar máscaras en público, pese a que nunca se detiene (ni se detendrá) a otras personas por ese tipo de infracción (pensemos en lo que ocurre en Halloween o durante una epidemia).

Tenemos razones más que fundadas para deshacernos de las leyes y las normas anacrónicas, pues pueden provocar injusticias y retrasar el progreso. Por eso las insinuaciones de Zuckerberg de que la privacidad se había vuelto obsoleta eran tan sugerentes. Desde entonces, llevado por el deseo de tranquilizar a los usuarios y de seguirles el ritmo a otros competidores que se toman más en serio la privacidad, Zuckerberg ha cambiado de idea y, en 2019,

afirmó que «el futuro es privado». [55] Solo un mes después, el abogado de Facebook defendió ante un tribunal que «la privacidad no es un interés de los usuarios» que se pueda vulnerar, pues, por el mero hecho de usar la plataforma, estos han «renunciado a toda expectativa razonable de privacidad». [56] Si Zuckerberg está en lo cierto y el futuro es privado, y si el abogado de Facebook tiene razón y los usuarios no pueden esperar privacidad alguna en esta plataforma, entonces la conclusión lógica parece ser que, en el futuro, habrá privacidad y Facebook no existirá.

No obstante, y pese a que Zuckerberg se haya desdicho de algunos comentarios previos, a la privacidad se la sigue culpando con reiterada insistencia de ser una traba para el progreso. Desde 2001, la privacidad ha sido acusada una y otra vez de representar un obstáculo en las iniciativas de las autoridades dirigidas a proteger a los ciudadanos. A la privacidad también se la trata con dureza en el contexto de la sanidad. Los médicos y las compañías tecnológicas ávidas de datos personales sostienen que es una barrera para el avance de la medicina personalizada y el análisis de macrodatos.

Durante la pandemia de coronavirus se ha hablado mucho de cómo una relajación en las normas sobre privacidad podría ayudar a atajar los brotes. En países de todo el mundo se han utilizado diversas apps de rastreo de contactos con el fin de identificar a personas que pudieran haber contraído la infección. Diferentes expertos estudiaron hasta qué punto las leyes de sus respectivos países dejaban un margen para introducir excepciones a la protección de datos en un contexto de pandemia. En un informe del Instituto Tony Blair para el Cambio Global, se defendía que el espectacular aumento de la vigilancia tecnológica era «un precio que vale la pena pagar» para luchar contra el coronavirus, aun cuando «no esté garantizado que ninguno de esos nuevos enfoques sea totalmente eficaz». [57]

Tan peligroso como conservar normas desfasadas es creer que ciertas normas cruciales han caído en la obsolescencia. La privacidad tiene una larga historia tras de sí. Podemos hallar rastros de normas protectoras de esta en casi todas las sociedades estudiadas hasta el momento. [58] A quienes afirman que la privacidad ha muerto, pídeles que te faciliten la contraseña de su cuenta de correo electrónico. O, mejor aún, la próxima vez que estés en unos aseos públicos, salúdales desde la cabina adyacente mientras les echas una miradita por debajo del panel de separación. Ya verás que no falla —las normas de privacidad siguen gozando de buena salud.

Puede que sea en la relativa eficacia con la que la privacidad ha logrado mantenerse con vida a lo largo del tiempo y en tantas culturas distintas donde le aceche su mayor peligro, ya que esto ha facilitado que la demos por sentada. Las

ventajas que nos brinda la privacidad se han mantenido lo bastante estables durante suficiente tiempo como para que podamos olvidar lo mucho que importa y por qué. Un fenómeno parecido se observa de forma habitual en el contexto de la salud pública. Cuando logramos evitar (o contener) con rapidez una epidemia, tendemos a subestimar la importancia de las medidas aplicadas —por ejemplo, cuando toca aplicarlas de nuevo ante otra amenaza de epidemia—, porque en su día no llegamos a sufrir los efectos negativos de lo que podría haber ocurrido si no hubiéramos intervenido a tiempo. De igual modo, podemos olvidarnos del valor de la privacidad si llevamos algún tiempo sin sentir las consecuencias de su pérdida. No es casualidad que en Alemania haya una mayor conciencia sobre la privacidad que en la mayoría de los países. El recuerdo de la Stasi, el servicio de seguridad estatal de la República Democrática Alemana, está muy vivo todavía.

Fuera del entorno digital, las señales que nos alertan de cuándo se ha violado una norma relacionada con la privacidad son, en general, muy palpables. Pocas sensaciones son tan incómodas socialmente como que otros te escudriñen cuando no quieres que te observen. Cuando alguien te roba tu diario privado, queda una ausencia. Si alguien te espía por la ventana, puedes pillarle in fraganti. La era digital ha conseguido que nos olvidemos de nuestras normas sobre privacidad, en gran parte porque ha logrado desligarlas de esas otras señales de intromisión más tangibles. El robo de datos digitales no nos crea ninguna sensación, no deja en nosotros un rastro visible, no hay una ausencia que percibir. La pérdida de privacidad en el entorno digital solo duele cuando tenemos que soportar sus consecuencias: cuando se nos niega un préstamo o un seguro, cuando se nos humilla o se nos acosa, cuando somos víctimas de una extorsión, cuando desaparece dinero de nuestra cuenta bancaria, o cuando nuestras democracias se debilitan.

Los dos capítulos siguientes son un recordatorio de dos lecciones importantes sobre privacidad que, muy probablemente, nuestros padres y abuelos comprendieron mejor que nosotros: una es que la batalla por nuestra privacidad es una lucha de poder, y la otra es que los datos personales son tóxicos.

3

Privacidad es poder

Imagina que tuvieras una llave maestra de tu vida. Una clave o contraseña que permite acceder a tu casa, a tu dormitorio, a tu diario, a tu ordenador, a tu teléfono, a tu coche, a tu caja fuerte, a tus historiales médicos. ¿Irías por ahí haciendo copias de esa llave y dándoselas a desconocidos? Probablemente no. Entonces ¿por qué estás dispuesto a entregar tus datos personales a casi cualquiera que te los pida?

La privacidad es la llave que abre la cerradura de tus aspectos más íntimos y personales, aquellos que te hacen más *tú* , y más vulnerable. Tu cuerpo desnudo. Tus fantasías y experiencias sexuales. Tus enfermedades pasadas y presentes, y aquellas que podrías tener en el futuro. Tus miedos, pérdidas y fracasos. Lo peor que hayas hecho, dicho o pensado nunca. Tus debilidades, errores y traumas. El momento en el que más vergüenza hayas pasado. Ese familiar que desearías no tener. La noche de tu peor borrachera.

Cuando das esa llave —tu privacidad— a alguien que te quiere, esta os abre la puerta a disfrutar de una mayor intimidad, y a que esa persona la use en tu beneficio. Parte de lo que significa tener una cercanía íntima con alguien es compartir aquello que te hace sentir vulnerable, darle el poder de hacerte daño, pero confiando en que esa persona nunca se aprovechará de la posición privilegiada que le confiere la intimidad. Las personas que te quieren tal vez utilicen tu fecha de nacimiento para organizarte una fiesta sorpresa de cumpleaños; puede que tomen nota de tus gustos para encontrarte el regalo perfecto; quizá tengan en cuenta cuáles son tus miedos más oscuros para protegerte de lo que más te asusta.

Sin embargo, no todo el mundo usará el acceso a tu privacidad para beneficiarte. Puede que un defraudador utilice tu fecha de nacimiento para hacerse pasar por ti y cometer algún delito en tu nombre; puede que una empresa use la información sobre tus gustos para tentarte a comprar o contratar algo que no te conviene; puede que un enemigo se valga de tus temores más oscuros para amenazarte y chantajearte. Las personas que no están interesadas en protegerte tratarán de sacar para sí un provecho de tus datos. Y a la mayoría de los individuos y las empresas con los que interactúas no les preocupan tus intereses, sino los suyos. La privacidad importa porque la falta de esta les da a otros poder

sobre ti.

Tal vez pienses que no tienes nada que esconder ni que temer. Te equivocas, salvo que seas un exhibicionista con deseos masoquistas de sufrir robos de identidad, discriminación, desempleo, humillaciones públicas y totalitarismos, entre otras desgracias. Tienes mucho que ocultar, mucho que temer, y el que no vayas por ahí haciendo públicas tus contraseñas o regalando copias de tus llaves a extraños lo demuestra.

Quizá pienses que tu privacidad está a salvo porque eres un don nadie y no hay nada especial, interesante o importante que descubrir sobre ti. No te subestimes. Si no fueras importante, las empresas y los gobiernos no se tomarían tantas molestias para espiarte.

Tienes el poder de tu atención, de tu interés por las cosas. Todos los actores del sector de las tecnológicas quieren que prestes atención a su app, a su plataforma, a sus anuncios. [1] Quieren saber más de ti para averiguar el mejor modo de distraerte, aunque eso implique que no pases tiempo de calidad con tus seres queridos o que no satisfagas necesidades básicas como el dormir. [2] Tienes dinero, por poco que sea. Las compañías quieren que te gastes en ellas lo que ganas. Los jáqueres que se han propuesto extorsionarte están deseosos de hacerse con tu información o tus imágenes sensibles. [3] También las aseguradoras quieren tu dinero, siempre que no representes un riesgo demasiado elevado para ellas —de ahí que anhelen tus datos para evaluarlo. [4] Tal vez estés en el mercado de trabajo. Las empresas quieren saberlo todo del personal al que contratan, incluyendo si eres de aquellos que están dispuestos a luchar por defender sus derechos. [5]

Tienes un cuerpo. Muchas instituciones, públicas y privadas, quieren saber más de él, quizá incluso experimentar con él, y quieren averiguar más sobre otros cuerpos como el tuyo. Tienes una identidad. Los delincuentes quieren usarla para cometer delitos en tu nombre y hacer que pagues el pato. [6] Tienes contactos y conexiones. Eres un nodo en una red. Eres descendiente de alguien, vecino de alguien, profesor, abogado o peluquero de alguien. A través de ti, se puede acceder a otras personas. Por eso las aplicaciones te piden acceso a tus contactos. Tienes una voz. Toda clase de agentes quieren usarla como altavoz en las redes sociales y más allá de estas. Tienes un voto. Fuerzas foráneas y nacionales quieren que votes al candidato que defenderá sus intereses. Como puedes ver, eres una persona muy importante. *Eres una fuente de poder* .

A estas alturas, la mayoría somos conscientes de que nuestros datos valen dinero. Sin embargo, tus datos no son valiosos solo porque se pueden vender. Técnicamente, Facebook, por ejemplo, no vende tus datos. [7] Tampoco lo hace Google. [8] Venden el poder de influir en ti. Guardan tus datos para poder vender

el poder de mostrarte anuncios y el de predecir tu conducta. Google y Facebook, en un sentido técnico, se dedican al negocio de los datos, pero su negocio más bien es el del poder. Más que una ganancia económica, los datos personales suministran poder a quienes los recopilan y analizan, y por eso son tan codiciados.

PODER

Lo único más valioso que el dinero es el poder. El poder puede conseguirte todo. Si posees poder, no solo puedes tener dinero, sino también la capacidad de salirte con la tuya en cualquier cosa que te propongas. Con suficiente poder, incluso puedes permitirte estar por encima de la ley.

El poder se caracteriza por dos aspectos. El primero es aquello que el filósofo Rainer Forst definió como «la capacidad de A para mover a B a pensar o hacer algo que, de lo contrario, B no habría pensado o hecho». [9] Las personas e instituciones poderosas pueden hacer que pienses y hagas cosas. Los medios a través de los que los poderosos hacen efectiva su influencia son diversos. Entre ellos se incluyen los discursos motivadores, las recomendaciones, los relatos ideológicos del mundo, la seducción y las amenazas creíbles. En la era digital, pueden contarse también entre los muchos medios por los que se ejerce poder los algoritmos clasificadores, las apps persuasivas, los anuncios personalizados, los bulos (*fake news*), los grupos y cuentas falsos, así como la reiteración de relatos que caracterizan las tecnologías como la solución a todos nuestros problemas. Es lo que llamamos «poder blando».

Forst sostiene que la fuerza bruta o la violencia no es un ejercicio de poder, pues las personas sometidas a ella no «hacen» nada, sino que, más bien, es a ellas a quienes se les hace algo. No estoy de acuerdo. La fuerza bruta es claramente un ejemplo de poder. Va contra el sentido común pensar que alguien que está ejerciendo violencia contra nosotros carece de poder. Imagina, si no, el caso de un ejército sometiendo a una población, o el de un matón estrangulando a alguien. Max Weber, uno de los fundadores de la sociología, describió este segundo aspecto del poder como la capacidad que unas personas o instituciones tienen «de imponer su propia voluntad aun contra toda resistencia». [10] Aquí lo llamaremos «poder duro».

En resumen, las personas y las instituciones poderosas hacen que nos comportemos y pensemos de forma diferente a como lo haríamos sin su influencia. Si no logran influir en nosotros para que actuemos y pensemos como quieren que lo hagamos, las personas e instituciones poderosas pueden recurrir

entonces a la fuerza; pueden hacer con nosotros lo que nosotros mismos no haríamos.

Existen diferentes tipos de poder: económico, político, militar, etcétera. El poder puede concebirse de manera análoga a la energía; puede transformarse de un tipo en otro. [11] Una empresa con poder económico puede utilizar su dinero para adquirir poder político mediante el cabildeo, por ejemplo. Una persona con poder político puede usarlo para ganar dinero intercambiando favores con compañías privadas.

Que gigantes tecnológicos como Facebook y Google son poderosos no es noticia. No obstante, examinar la relación entre la privacidad y el poder puede ayudarnos a entender mejor cómo las organizaciones amasan, manejan y transforman el poder en la era digital, lo que a su vez puede darnos herramientas e ideas que nos permitan resistir con mayor eficacia a la forma de dominación propiciada por las violaciones del derecho a la privacidad. Para llegar a comprender a fondo cómo las organizaciones acumulan y ejercen el poder en la era digital, primero tendremos que examinar la relación entre el poder y el conocimiento.

Poder y conocimiento

Hay una estrecha conexión entre el poder y el conocimiento. Para empezar, el conocimiento es un instrumento del poder. El filósofo inglés Francis Bacon comprendió que el conocimiento en sí es una forma de poder. Más de tres siglos después, el filósofo e historiador de las ideas francés Michel Foucault fue aún más lejos y argumentó que tan cierto es que el poder produce conocimiento como a la inversa. [12] Saber comporta poder, y tener poder comporta saber. El poder crea conocimiento y decide qué se considera como tal. Recopilando tus datos y aprendiendo cosas sobre ti, Google se empodera, y ese poder le permite decidir, a través de su uso de tus datos personales, qué conocimientos relativos a ti son válidos. Si Google te clasifica como un hombre de mediana edad sin carrera universitaria y aquejado de ansiedad, por poner un ejemplo, eso es lo que se considerará como conocimiento válido sobre ti, aunque sea totalmente erróneo, o fuera de contexto, o desfasado, o irrelevante. Protegiendo nuestra privacidad, impedimos que otros se empoderen con un conocimiento relativo a nosotros que pueda usarse en contra de nuestro interés. Disponiendo de mayor poder, tenemos más influencia para determinar qué conocimiento se considerará válido. Deberíamos poder decidir (en parte, al menos) qué conocimiento referente a nosotros es el que vale; deberíamos tener algo que decir a propósito

de qué es lo que otros pueden percibir o inferir sobre nosotros.

Cuanto más sabe alguien de nosotros, más puede prever nuestros movimientos e influirnos. Una de las aportaciones más importantes de Foucault a nuestra visión del poder es la idea de que el poder no solo actúa sobre las personas, sino que también construye sujetos humanos. [13] El poder genera ciertas mentalidades, transforma sensibilidades, crea unos modos de estar en el mundo. En la misma línea, el teórico político y social Steven Lukes sostiene que el poder puede producir un sistema que genere deseos en las personas que van en contra de sus intereses. [14]

Los propios deseos de la gente pueden ser resultado del poder y, cuanto más invisibles son los medios por los que este actúa, más poderosos resultan. Un ejemplo de cómo el poder conforma las preferencias es cuando las tecnológicas usan investigaciones sobre la dopamina para generarte adicción a una aplicación. La dopamina es un neurotransmisor que te motiva a actuar a través de la anticipación que te genera pensar en satisfacer tus deseos. Imaginarte lo bien que sabrá un pastel de chocolate te mueve a comprarlo y comerlo. Anticipar lo reafirmado que te sentirás cuando tus amigos elogien tu aspecto te motiva para hacerte un selfiy compartirlo en línea. Las compañías tecnológicas usan tácticas como la creación de recompensas a intervalos irregulares (que es lo que hace que las máquinas tragaperras sean tan adictivas) o la utilización de colores llamativos para que sus plataformas absorban al máximo tu atención. Los «me gusta» y los comentarios que recibes por tus publicaciones te «producen un ligero golpe de dopamina». [15] Tus ganas de usar una app persuasiva no nacen de tus valores y compromisos más profundos. Lo normal es que no te despiertes por la mañana pensando «hoy quiero pasarme tres horas tontas repasando la interminable sección de noticias de mi cuenta de Facebook». Ese deseo solo te viene inducido por el poder de la tecnología. En ese sentido, no es del todo tuyo. Otro ejemplo son las campañas políticas que investigan tus inclinaciones afectivas y cognitivas para mostrarte un anuncio que te empuje a actuar como quieren que lo hagas.

Tanto el poder derivado del saber como el conocimiento definido por el poder pueden ser más dominantes cuando existe una asimetría de conocimiento entre las dos partes. Si, por ejemplo, Facebook sabe todo lo que hay que saber sobre ti, y tú no sabes nada sobre Facebook, entonces la tecnológica tendrá más poder sobre ti que si ambas partes supierais más o menos lo mismo una de otra. La asimetría se vuelve más pronunciada si Facebook lo sabe todo de ti y tú crees que no sabe nada (o desconoces lo mucho que sabe). Eso te convierte en ignorante por partida doble.

El poder que resulta de conocer detalles personales sobre alguien es un tipo de poder muy particular, pero también brinda a quienes lo tienen la posibilidad de

transformarlo en un poder económico, político o de otra clase.

El poder en la era digital

El poder de pronosticar e influir que se deriva de los datos personales es el poder por antonomasia en la era digital.

Nunca los gobiernos supieron tanto de sus ciudadanos. La Stasi, por ejemplo, solo llegó a tener expedientes de aproximadamente un tercio de la población de la Alemania del Este, por mucho que aspirara a poseer información completa sobre toda la ciudadanía. [16] Las agencias de inteligencia actuales manejan cantidades mucho mayores de información referente a toda la población. Para empezar, una proporción significativa de la gente facilita de manera voluntaria información privada a través de las redes sociales. En palabras de la documentalista Laura Poitras, «Facebook es un regalo para las agencias de inteligencia». [17] Entre las posibilidades que abre esa clase de información, está la de dar a los gobiernos la capacidad de adelantarse a las protestas y practicar arrestos preventivos. [18] Poder conocer cuál será la resistencia organizada antes de que esta se produzca y aplastarla a tiempo es el sueño de cualquier tiranía.

El poder de las compañías tecnológicas se forma, por un lado, a partir de la posesión de un control exclusivo sobre nuestros datos y, por otro, por su capacidad de prever todos nuestros movimientos, lo que, a su vez, les brinda múltiples oportunidades de influir en nuestra conducta y de vender esa influencia a otros, gobiernos incluidos.

Parte de la razón por la que las grandes tecnológicas nos tomaron por sorpresa fue que sus métodos escaparon al radar de las autoridades antimonopolio. Estamos acostumbrados a medir el poder de las empresas en términos económicos, es decir, en función de lo que cobran a sus usuarios. Sin embargo, el poder de las grandes tecnológicas proviene de los datos personales que se llevan, no de lo que cobran. Tradicionalmente, el síntoma más habitual de que una compañía merecía una atención especial de los organismos antimonopolio era que podía aumentar precios sin perder clientes. Como Google y Facebook proporcionan servicios «gratuitos», esa regla heurística no funciona. La prueba de fuego tradicional debería entenderse como un ejemplo particular de un principio más general: si una empresa puede maltratar a sus clientes sin perderlos (cobrándoles por encima de lo que sería un precio justo, aplicándoles prácticas explotadoras con sus datos, descuidando la seguridad o imponiéndoles cualesquiera otras condiciones abusivas), entonces es muy probable que sea un monopolio.

Unas compañías cuyos ingresos provienen mayoritariamente de la publicidad se han valido de nuestros datos para crearse un foso protector a su alrededor —una ventaja competitiva que ha imposibilitado que otras empresas alternativas desafíen a esos titanes tecnológicos. [19] El buscador de Google, por ejemplo, es tan bueno en parte porque su algoritmo cuenta con muchos más datos de los que aprender que cualquiera de sus competidores. Además de mantener a la compañía protegida de la competencia y de ayudarla a entrenar a su algoritmo, semejante volumen de datos permite que Google sepa qué te quita el sueño, cuál es tu mayor deseo, qué tienes previsto hacer a continuación, o sobre qué estás dudoso. La empresa se encarga luego de cuchichearle esa información a otros entrometidos interesados en dirigirte publicidad personalizada.

Los buitres de datos tienen una increíble destreza en el manejo de los dos aspectos del poder aquí comentados: hacen que les entreguemos nuestros datos de manera más o menos voluntaria y también nos los roban cuando tratamos de resistirnos.

El poder duro de las tecnológicas

Cuando se nos arrebatan datos aunque intentemos oponernos, somos víctimas del poder duro de la tecnología. Ocurre, por ejemplo, cuando Google almacena datos sobre ubicación incluso después de que le hayamos indicado que no lo haga: en una investigación realizada en 2018, Associated Press descubrió que Google seguía guardando datos de ese tipo aun después de que los usuarios hubieran desactivado el historial de ubicaciones. En la página de ayuda de la tecnológica podía leerse lo siguiente: «Puedes desactivar el historial de ubicaciones en cualquier momento. Cuando este está desactivado, dejan de guardarse los lugares donde has estado». No era verdad. Google Maps, por ejemplo, almacenaba de manera automática una instantánea de tu latitud y tu longitud en el momento en que abrías la app, aunque ya hubieras apagado tu historial de ubicaciones. Algo parecido ocurría con algunas búsquedas no relacionadas con dónde te encontraras en ese momento —por ejemplo, «receta de galletas con pepitas de chocolate»—, que guardaban tu ubicación en tu cuenta de Google. Para apagar los marcadores de ubicación, tenías que desactivar una recóndita opción de configuración en la que no se mencionaba la ubicación (la «actividad en la web y en aplicaciones») y que —cómo no— estaba activada por defecto y guardaba en tu cuenta información de las apps de Google y de otros sitios web. [20]

El poder duro de las tecnológicas puede confundirse a veces con poder blando

porque no parece tan violento como otras manifestaciones conocidas del primero, como los tanques por las calles y el empleo de la fuerza bruta. Sin embargo, el que alguien te haga aquello a lo que has dicho que «no» es poder duro. Es algo que se te impone a la fuerza y que vulnera tus derechos.

Aunque el poder duro ha sido consustancial a las tecnológicas desde el principio, pues siempre se han llevado nuestros datos sin pedir permiso antes, sus métodos se están volviendo cada vez menos sutiles y más manifiestamente autoritarios. China es un ejemplo destacado. Hace años que el Gobierno chino diseña y perfecciona un sistema de crédito social con la colaboración de empresas tecnológicas. Se trata de un sistema que traduce y exporta el concepto de «solvencia económica» a todos los demás ámbitos de la vida con la ayuda de los macrodatos. Todos los datos de cada ciudadano se utilizan para puntuar a esa persona conforme a una escala de fiabilidad. Los «buenos» actos de un individuo le hacen ganar puntos, mientras que los «malos» hacen que los pierda. Comprar pañales cosecha puntos. Jugar con la consola, comprar alcohol o difundir bulos te quita puntos.

Una de las características de las sociedades totalitarias es que el poder controla todos los aspectos de la vida: de ahí que sea «total». En las democracias liberales (en su mejor versión), una persona no se ve penalizada en todos los ámbitos de su vida por las pequeñas infracciones cometidas en una esfera. Por ejemplo, si pones la música alta en casa, puedes ganarte el odio de los vecinos, y puedes incluso provocar alguna visita de la policía en la que los agentes te pidan que bajes el volumen, pero eso no tendrá ningún efecto en tu vida laboral o en tu calificación crediticia (a menos que tengas la mala fortuna de que el vecino afectado sea tu jefe o tu banquero). En China, poner alta la música, cruzar la calle por sitios no señalizados para ello o hacer trampas en un videojuego haría que perdieras puntos en una calificación que se usaría luego para concederte o restringirte oportunidades en todas las esferas de la vida.

Los ciudadanos con altas puntuaciones a veces reciben algún tipo de elogio público y disfrutan de ciertas ventajas, como listas de espera más cortas o descuentos en la compra de productos y servicios como habitaciones de hotel, recibos del agua o la luz, o préstamos. Pueden alquilar un vehículo sin pagar una fianza, e incluso tienen una mayor visibilidad en sitios de citas. Los ciudadanos con una puntuación baja pueden ser humillados públicamente y les puede resultar difícil (o imposible) encontrar trabajo, contratar un préstamo o comprar una propiedad inmobiliaria; también se les puede incluir en listas negras que veten su acceso a servicios como hoteles exclusivos o que incluso les impidan viajar en avión o en tren.

En 2018, China avergonzó a ciento sesenta y nueve personas «gravemente

desacreditadas» publicando sus nombres y sus fechorías, entre las que se incluían cosas como haber intentado pasar un mechero de bolsillo por un control de seguridad de un aeropuerto, o haber fumado en un tren de alta velocidad. [21] Según el documento fundacional del sistema, este aspira a «permitir que las personas dignas de confianza puedan ir adonde quieran y, al mismo tiempo, dificultar que los desacreditados puedan dar un solo paso». [22] Hasta el final de junio de 2019, China había prohibido ya a casi 27 millones de personas la compra de billetes de avión, y a casi 6 millones viajar por la red ferroviaria de alta velocidad. [23] Durante la pandemia de coronavirus, la vigilancia china llegó al extremo de instalar a la fuerza cámaras en el interior de domicilios particulares (o en el exterior de las puertas de entrada de estos) para asegurarse de que la población cumplía con las normas del confinamiento. [24]

Cuando los occidentales critican el régimen chino de disciplina social, una de las réplicas habituales es que Occidente también ha implantado sistemas en los que las personas reciben puntuaciones y pueden ser penalizadas en función de estas, pero con el agravante de que los sistemas occidentales de crédito social son más opacos. A menudo los ciudadanos desconocen hasta su existencia. Es una respuesta no exenta de verdad. Normalmente, no somos muy conscientes de cómo se calcula nuestra puntuación crediticia ni de qué uso se le puede estar dando, por ejemplo. También hay otros tipos de puntuación. La mayoría de las personas no lo saben, pero, como consumidor, tienes unas puntaciones secretas que determinan cuánto tiempo te toca esperar cuando llamas al teléfono de un comercio o una empresa, o si puedes devolver a una tienda artículos que has comprado, o la calidad del servicio que recibes. Y ni siquiera tienes la opción de renunciar a que te califiquen como consumidor; es algo que te viene impuesto.

La periodista Kashmir Hill solicitó su expediente a Sift, una compañía estadounidense especializada en calificar a consumidores. Este consistía en 400 páginas llenas de años de pedidos realizados a través de Yelp, de mensajes enviados por Airbnb, de detalles sobre sus dispositivos, y mucha más información. Aunque Sift atendió su solicitud y le facilitó los datos personales que de ella tenía, no le ofreció explicación alguna de cómo los analizaba para generar su puntuación como consumidora, ni le especificó qué consecuencias había tenido esa calificación para su vida. [25]

Los sistemas de calificación secretos y opacos son inaceptables. Como ciudadanos, tenemos derecho a saber las normas que rigen nuestras vidas. No obstante, es innegable que, en general, Occidente disfruta de un mayor grado de libertad y transparencia que China, pese a nuestras deficiencias en gobernanza (que deberíamos esforzarnos por rectificar). [26] Que nuestras faltas y las de los demás nos sirvan de lecciones para aprender a poner freno al poder duro que nos

rodea.

Otra forma en la que la tecnología puede ejercer el poder duro es fijando las reglas conforme a las que vivimos e impidiéndonos romperlas. En vez de tener normas fijadas en su mayor parte por escrito, hoy cada vez más tenemos normas incorporadas en el código de los programas informáticos e impuestas de manera automática por los ordenadores. [27] Es posible, pues, que tu futuro coche no te permita conservar la libertad de conducir por un carril bus —y de arriesgarte a que te pongan una multa—, porque simplemente se niegue a ir por donde esté prohibido. [28]

En las sociedades libres, siempre existe cierto margen de maniobra entre lo que se estipula en las leyes y su aplicación en la realidad. Las personas pueden salir impunes de ciertas infracciones menores ocasionales porque, en las sociedades que funcionan bien, la mayoría de la gente está conforme con obedecer la mayoría de las normas durante la mayor parte del tiempo. [29] Ese margen de flexibilidad permite encajar excepciones que resultarían difíciles de regular, como, por ejemplo, el que un vehículo no autorizado circule por el carril bus cuando está trasladando a un herido grave al hospital. También nos permite hacer caso omiso de leyes obsoletas y aún pendientes de revocación. Si las leyes fueran implementadas por ordenadores, no cabrían excepciones. El poder duro que ejercería la tecnología al imponer de forma implacable todas las normas —estatales o privadas— inscritas en el código informático nos privaría de un enorme grado de libertad.

Pero la tecnología no solo utiliza el poder duro para influir en nosotros. Se le da de maravilla influir en nosotros por medio del poder blando.

El poder blando de las tecnológicas

En ciertos sentidos, el poder blando es más aceptable que el duro porque es menos contundente. No parece imponerse con tanta fuerza. Sin embargo, el poder blando puede ser tan eficaz como el duro ayudando a los poderosos a conseguir lo que quieren. Además, el poder blando suele ser manipulador; consigue que hagamos algo en beneficio de otros con el pretexto de que lo hacemos en nuestro propio beneficio. Se sirve de nuestra voluntad para usarla contra nosotros. Bajo la influencia del poder blando, nos comportamos de formas que no son las que más nos convienen.

El poder blando manipulador nos hace cómplices de nuestra propia victimización . [30] Es *tu* dedo el que va desplazándote hacia abajo por más y más publicaciones de la red social, haciéndote perder un valioso tiempo y

dándote un dolor de cabeza. Pero, claro, no estarías enganchado a ese *scrolling* infinito si plataformas como Facebook no se esforzaran tanto por convencerte de que, de no seguir mirando más abajo, te estarías perdiendo algo importante. Cuando tratas de resistirte a la cautivadora atracción de esas tecnologías, luchas contra un ejército de informáticos empeñados en captar tu atención más allá de lo que te conviene.

Las «tarjetas cliente» son un ejemplo más de poder blando. Cuando en el supermercado te ofrecen una tarjeta de fidelidad, lo que te proponen en realidad es la oportunidad de que des permiso a esa empresa para que te vigile y, de paso, influya en tu comportamiento (induciéndote con descuentos, por ejemplo) para que compres ciertos productos que, de otro modo, no adquirirías.

Una forma más sutil de poder blando es la seducción. Las tecnológicas nos seducen de forma continua para que hagamos cosas que de lo contrario no haríamos, como perdernos en un laberinto de vídeos en YouTube, jugar juegos sin sentido, o mirar nuestros teléfonos cientos de veces al día. Con toda una serie de tentadoras «zanahorias», la era digital ha traído consigo nuevos modos de estar en el mundo que no siempre mejoran nuestras vidas.

Aparte de las vías técnicas para el ejercicio de un poder blando prediseñado, gran parte del poder de las tecnológicas radica en los «relatos», en las historias que se cuentan sobre nuestros datos. La economía de los datos ha logrado normalizar ciertas maneras de pensar. Las compañías tecnológicas quieren que creas que, si no has hecho nada malo, no tienes motivos para oponerte a que conserven la información que recopilan sobre ti. Cuando le preguntaron en una entrevista a Eric Schmidt, el entonces director ejecutivo de Google, si los usuarios debían compartir información con su empresa respondió de forma célebre: «Si tienes algo que no quieres que se sepa, a lo mejor no deberías haberlo hecho». [31] (No tan conocido es que él mismo pidió a Google en una ocasión que borrara cierta información sobre él de los índices... y que la empresa le denegó la solicitud. [32] ¿Percibes cierto patrón en lo mucho que los *techies* parecen querer privacidad para sí mismos pero no para los demás?)

Lo que Schmidt intentó hacer fue avergonzar a las personas que (con muy buen juicio) se preocupan por la privacidad. Dio a entender que, si te preocupa la privacidad, será porque tienes cosas que ocultar, y que, si tienes cosas que ocultar, será porque has hecho algo malo que no debería permitírsete mantener oculto. Sin embargo, el valor de la privacidad no tiene que ver con esconder delitos graves. [33] Su finalidad, más bien, es protegernos de los demás, como, por ejemplo, de los delincuentes que quieren robarnos dinero. Sirve para vendarle los ojos al poder e impedir que use lo que vaya averiguando de nosotros para hacerse más poderoso todavía.

Las compañías también quieren que pienses que tratar tus datos como si fueran una mercancía es *necesario* para el funcionamiento de la tecnología digital, y que la tecnología digital es el *progreso* , aunque en ocasiones pueda tener una preocupante semejanza a la regresión social y política. [34] Pero, sobre todo, las tecnológicas quieren que pienses que las innovaciones que sacan al mercado son *inevitables* : [35] así es el progreso y este no se puede detener.

El relato sobre la tecnología como un progreso inevitable es tan complaciente como engañoso. El poder produce el conocimiento, los relatos y la racionalidad que más lo favorecen y sustentan. [36] Las tecnológicas nos cuentan aquellas historias que las presentan como indispensables y buenas. Sin embargo, parte de la tecnología que se ha desarrollado en las últimas décadas no ha representado progreso alguno; más bien ha contribuido a perpetuar tendencias sexistas y racistas. [37]

Cuando el traductor de Google pasa noticias del español al inglés, «ella» suele convertirse en «él». Se sabe que los algoritmos refuerzan las analogías sexistas —que para ellos «hombre» es a «médico» o a «programador informático» lo que «mujer» es a «enfermera» o a «ama de casa», por poner dos ejemplos. [38] Los algoritmos de visión asignan a las nupcias de una contrayente blanca las etiquetas «novia», «mujer» y «boda», pero cuando se trata de la fotografía de una novia del norte de la India los conceptos asignados son «*performance* artística» y «disfraz». El Banco Mundial ya ha advertido de que Silicon Valley está agravando la desigualdad de renta. [39] Un cambio tecnológico que nos conduzca al retroceso social y político no es el tipo de desarrollo que deberíamos perseguir ni impulsar. Esto *no* es progreso.

Además, ninguna tecnología es inevitable. Nada estaba escrito de antemano en la historia, en la naturaleza o en el destino que hiciera que la llegada de los automóviles con motor de combustión fuese ineludible, por ejemplo. Si no se hubieran descubierto unas enormes reservas de petróleo en Estados Unidos, y si Henry Ford no hubiera fabricado el económico Modelo T, los coches eléctricos podrían haber terminado siendo mucho más populares. [40] Y, aunque hace décadas que se habla de los coches voladores, es posible que jamás lleguen a ser una realidad. Que una tecnología concreta se desarrolle y se comercialice depende de toda una serie de variables relacionadas con la viabilidad, el precio y la elección humana. Los vertederos de la historia están llenos de cachivaches tecnológicos que pasaron a mejor vida antes de hacer fortuna.

¿Te acuerdas de Google Glass? En 2013, Google comenzó la venta limitada de un prototipo de gafas que llevaban integrado un diminuto ordenador e incluían también una cámara de vídeo. Se pusieron a la venta para el público general en mayo de 2014. Fue un producto al que se le dio mucho bombo en los medios. La

revista *Time* lo incluyó entre los «mejores inventos del año». Muchos famosos se las probaron. *The New Yorker* dedicó un largo artículo al invento. Llegaron incluso a protagonizar un episodio de *Los Simpson* (aunque Homer las llamó «Oogle Goggles»). A pesar del alboroto generado por su lanzamiento, en enero de 2015 el producto ya había sido retirado del mercado. [41] (En vez de admitir su derrota, Google dijo que había procedido a «graduar» sus gafas inteligentes transfiriéndolas de una de sus divisiones empresariales a otra.)

El estrepitoso fracaso de Google Glass se debió, por lo menos, a dos razones. En primer lugar, las gafas eran horribles. Y, en segundo (y más importante) lugar, inspiraban temor. Antes incluso de que nadie se las hubiera visto puestas a otra persona, se prohibió su uso en bares, cines, casinos y otros sitios en los que la idea de que los clientes se grabaran unos a otros no despertaba ninguna simpatía. [42] Las pocas personas que se las probaron recibieron el descalificador mote de *glassholes* (del inglés *assholes* , «imbéciles»), toda una señal de la incomodidad que esos aparatos suscitaban en la población.

Google Glass no tuvo mayor recorrido porque la gente odiaba aquellas gafas; pero Google es una compañía tozuda. En 2017, resucitó el proyecto, aunque esta vez orientado a sectores como el de los servicios industriales, para su uso entre los trabajadores. No sería de extrañar que algún día Google intentara relanzar Glass para el público general. Desde 2013, esta y otras empresas han ido corroyendo de manera continua y consciente tanto nuestra privacidad como nuestra resistencia a las invasiones de esta. El Proyecto Aria de Facebook persigue el objetivo de sustituir los teléfonos inteligentes por gafas inteligentes. [43] Pero no debemos olvidar que el éxito de cualquier tecnología, como el de todas las demás prácticas sociales, depende de nuestra cooperación. Somos la fuente última de poder para las compañías tecnológicas.

El desarrollo tecnológico no es en absoluto un fenómeno natural como la gravedad o la evolución. *La tecnología no es algo que nos ocurra; somos nosotros quienes hacemos que ocurra* . [44] Unas gafas Google Glass no se inventan y se comercializan solas. Tampoco se generan por casualidad, como las mutaciones. [45] De nosotros depende asegurarnos de que nuestra tecnología se ajuste a nuestros valores y mejore nuestro bienestar. Que el progreso tecnológico sea inevitable suena a verdad porque lo que está claro es que siempre se va a producir algún tipo de cambio tecnológico, pero ninguna tecnología en particular es ineludible; además, «cambio» no siempre significa «progreso». Siempre podemos elegir cómo usar y regular una tecnología.

Un relato más veraz que el promovido por las tecnológicas es que podemos —y debemos— frenar aquellos desarrollos tecnológicos cuyas consecuencias negativas superen las positivas. A propósito de la privacidad, un relato más

ajustado a la realidad es que tratar los datos como mercancías es una manera que las empresas tienen de ganar dinero y en absoluto guarda relación con el objetivo de fabricar buenos productos. El acaparamiento de datos es el medio del que las instituciones se están valiendo para acumular poder. Las compañías tecnológicas pueden —y deben— esforzarse más por diseñar un mundo digital que contribuya al bienestar de las personas. Y tenemos muchas buenas razones para oponernos a que todas esas organizaciones recopilen y utilicen nuestros datos, aunque no hayamos hecho nada malo.

Entre esos motivos está el que estas instituciones no respeten nuestra autonomía —nuestro derecho a autogobernarnos—, ni como individuos ni como sociedad. [46] Es ahí donde el lado más duro del poder juega su papel. La era digital se ha caracterizado hasta el momento por la existencia de unas organizaciones que hacen lo que quieren con nuestros datos, saltándose sin escrúpulos el pedir nuestro consentimiento si creen que pueden salir impunes de ello, y, además de presionarnos a hacer lo que quieren que hagamos, nos imponen condiciones. Fuera del mundo digital, esa manera de comportarse se calificaría de robo y de coacción. Que no se la denomine así en el entorno virtual es una prueba más del poder de las tecnológicas sobre los relatos dominantes.

Si los empleados de los servicios postales leyeran nuestras cartas como Gmail y algunos terceros (desarrolladores de apps) han analizado nuestros correos electrónicos, irían a la cárcel. [47] La misma geolocalización en vivo que, en otros tiempos, se reservaba a los convictos, se ha convertido ahora en la norma en los teléfonos inteligentes que todos llevamos con nosotros. [48] Parte de por qué los impulsores de malas tecnologías se han salido con la suya hasta el punto en que lo han hecho se debe a que han hallado formas aceptables de describir lo que hacen. La mala tecnología explota nuestros datos, secuestra nuestra atención y fractura nuestras democracias, pero sus promotores hacen que todo eso suene apetecible, como si lo estuvieran haciendo por nuestro propio bien, como parte de una optimización de la «experiencia del usuario». La «personalización» suena a trato VIP, hasta que te das cuenta de que no es más que una forma de denominar técnicas diseñadas para manipular las mentes singulares de cada uno de nosotros.

En vez de llamar a las cosas por su nombre, las compañías tecnológicas nos han inundado de eufemismos sobre nuestras realidades digitales. [49] Tal y como escribió George Orwell a propósito del lenguaje político (y el lenguaje tecnológico es político), este «está diseñado para que las mentiras suenen a verdad y los asesinatos parezcan algo respetable; para dar aspecto de solidez a lo que es puro humo». [50] Unas redes de publicidad y vigilancia que son propiedad de empresas privadas reciben el nombre de «comunidades», los

ciudadanos son «usuarios», a la adicción a las pantallas se la cataloga como «compromiso» (*engagement*), a nuestra información más sensible la llaman «datos de escape», o «migas de pan digitales», y a los programas espías, «*cookies* », mientras que los documentos en los que se describe nuestra falta de privacidad se presentan con el título de «políticas de privacidad», y lo que solíamos considerar escuchas telefónicas son hoy la piedra fundacional de la economía de internet.

Las tecnológicas han llegado tan lejos seduciéndonos con las palabras que incluso han hecho suyo el lenguaje de la naturaleza. [51] Antes una manzana (*apple*) era algo cuya dulzura podíamos saborear, igual que podíamos escuchar el piar (*tweet*) de los pájaros al alba, o podíamos caminar con los pies metidos en la corriente (*stream*) de un arroyo y distinguir formas en las *nubes* al pasar. Ahora esas palabras se utilizan sobre todo para describir cosas que son lo contrario de la naturaleza.

A quienes nos dedicamos a pensar y a escribir nos corresponde desafiar todas esas sandeces corporativas y recuperar el lenguaje transparente. Llamar a las cosas por su nombre es un buen primer paso para entender mejor nuestros tiempos y luchar por un mundo mejor. Tenemos que construir nuestros propios relatos y usar las palabras que las tecnológicas intentan camuflar o evitar. Tenemos que reivindicar el poder de decidir qué es conocimiento y qué no. Hablemos sobre lo que las tecnológicas no quieren que hablemos. Por ejemplo, hablemos de cómo nos está tratando la mala tecnología: no como ciudadanos, sino como peones en una partida que nunca elegimos jugar. La mala tecnología nos utiliza a nosotros mucho más de lo que nosotros la utilizamos a ella.

PEONES

Eres un peón en los juegos que los científicos de datos juegan en sus pantallas. A veces lo llaman «sociedad artificial». Reúnen toda la información posible sobre ti —contactos y publicaciones en redes sociales, historiales de votaciones y de compras, la marca y el modelo de tu coche, tu información hipotecaria, tu historial de navegación, ciertas inferencias sobre tu salud, etcétera— y luego aplican modelos para ver cómo pueden influir en tu conducta.

Y me refiero a *ti* en particular. No importa si eres un don nadie: la sociedad la formamos donnadies y es en nosotros en quienes las organizaciones e instituciones hambrientas de datos están interesadas. Cuando un amigo mío estudiaba para ser científico de datos, me confesó que el último ejercicio que le habían pedido hacer había sido elegir a una persona al azar de un lugar

cualquiera del mundo y aprender todo lo que pudiera sobre ella. Terminó estudiando a fondo a un tipo de Virginia que, según averiguó, padecía diabetes y estaba teniendo una aventura. Ese individuo aleatorio no tenía ni la más remota idea de que estaba siendo objeto de estudio de un científico de datos en formación. En este mismo instante en que estás leyendo estas palabras, otro podría estar estudiándote a *ti* .

En cierto sentido, cada uno de nosotros tiene incontables clones en forma de datos que viven en los ordenadores de científicos de datos que están experimentando con nosotros, con diferentes grados de personalización. Los analistas juguetean con nuestros avatares virtuales como si estos fueran muñecos de vudú. Prueban novedades con ellos y ven qué pasa. Quieren aprender qué nos motiva (a hacer clic, comprar, trolear, votar...). Cuando aprenden a manipular de forma efectiva nuestros clones digitales cual marionetas, prueban sus trucos en personas de carne y hueso. Así es como nuestros zombis virtuales se vuelven contra nosotros.

Estos aspirantes a dioses de la tecnología estarían encantados de elaborar perfiles de todas y cada una de las personas de una sociedad para poder realizar simulaciones de esa comunidad. Si conoces suficientemente bien las personalidades de los individuos, puedes crear duplicados zombis de estos en línea y probar con ellos diferentes intervenciones. Puedes averiguar qué mensajes políticos funcionan con ellos. Y, cuando estás seguro de que un mensaje determinado provocará las consecuencias buscadas, puedes lanzarlo al mundo. Manipulando información, se pueden inclinar unas elecciones, inspirar una insurrección, prender la chispa inicial de un genocidio, enfrentar a las personas entre sí, distorsionar sus realidades hasta que ya no puedan distinguir entre lo que es verdad y lo que no.

Eso es justo lo que Cambridge Analytica hizo para ayudar a algunas campañas electorales. Para empezar, unos científicos de datos desarrollaron una app llamada «Esta es tu vida digital» y consiguieron que 270.000 usuarios de Facebook se la descargaran. Pagaron a cada persona entre uno y dos dólares por rellenar una encuesta psicométrica que ayudaba a los analistas a evaluar sus tipos de personalidad. La aplicación descargaba a continuación todos los datos de Facebook de los usuarios para poder buscar en ellos correlaciones entre, por ejemplo, sus rasgos de personalidad y sus «me gusta». Facebook es un objeto de estudio atractivo para las ciencias sociales porque, cuando las personas se desplazan por sus contenidos y hacen clic en «me gusta» y comentan, no son conscientes de hasta qué punto las están vigilando, por lo que actúan de forma más «natural». Los científicos de datos que observan cómo nos manejamos en (lo que deberían ser) nuestros asuntos se sienten como antropólogos, aunque con

la ventaja de poder cuantificar con facilidad hasta el último detalle. [52]

La aplicación de Cambridge Analytica también descargaba datos de los amigos que los participantes tenían en Facebook sin que aquellos lo supieran ni hubieran dado su consentimiento. [53] Aunque los científicos de datos no tenían los rasgos de personalidad de esos «sujetos de datos» que no sabían que lo eran (porque no habían respondido la encuesta psicométrica), podían usar sus «me gusta» de Facebook para deducirlos a partir de los estudios realizados con los datos de las personas que sí habían respondido la encuesta.

En resumidas cuentas, Cambridge Analytica embaucó a 270.000 personas para que traicionaran a sus amigos —y a varias democracias de todo el mundo— por apenas un dólar. Aunque los participantes respondieron de forma voluntaria la encuesta, lo más probable es que la mayoría no leyeran todos los términos y condiciones, entre los cuales, en cualquier caso, no se incluía advertencia alguna sobre cómo se iban a usar sus datos para tratar de influir en las elecciones. Valiéndose de los contactos de las personas para descargar el máximo de información privada posible, la empresa se hizo con los datos de unos 87 millones de usuarios de Facebook. También adquirieron otros adicionales que tomaron de censos y brókeres de datos, entre otras fuentes. Con todos esos datos, Cambridge Analytica fabricó una herramienta de guerra psicológica para influir en la política de todo el mundo; un ejemplo de manual de cómo el conocimiento es poder.

Cambridge Analytica escarbó a fondo en la vida y en la mente de los individuos. Los datos personales de los que se apropió eran de suma sensibilidad. Incluían mensajes «privados», por ejemplo. Y lo que los analistas hicieron con esos datos fue muy íntimo y personal. «Datos de millones de personas» suena muy impersonal y abstracto, pero cada uno de esos seres humanos es igual de real que tú. Tus datos podrían estar incluidos entre los de esos millones.

Christopher Wylie es un consultor de datos que trabajaba en Cambridge Analytica hasta que decidió denunciar públicamente las prácticas de la empresa desde dentro. En su libro, *Mindf*ck* , describe una demostración de la herramienta que la compañía dio a Steve Bannon, que posteriormente se convertiría en director ejecutivo de la campaña de Donald Trump. [54] Un científico de datos pidió a Bannon que le dijera un nombre y un estado de Estados Unidos. Con aquella simple consulta, la vida entera de una persona apareció en pantalla. Si esta hubieras sido tú (y tal vez lo fueras), ese grupo de científicos de datos habrían estado examinando tu vida con lupa: este es tu aspecto, ahí es donde vives, estos son tus mejores amigos, ahí es donde trabajas, ese es el coche que conduces. Votaste por tal o cual candidato en las últimas

elecciones, tienes esta hipoteca o aquella, tienes este problema de salud, detestas tu trabajo, este es el tema político que más te preocupa y estás pensando en dejar a tu pareja.

Para asegurarse de que estaban acertando en todo, los científicos de datos llamaron a continuación a la persona que estaban desnudando en pantalla. Haciéndose pasar por unos investigadores de la Universidad de Cambridge que estaban realizando una encuesta, formularon a su víctima preguntas sobre nombres, opiniones y estilo de vida. Las llamadas telefónicas confirmaron lo que ya sabían: habían diseñado una herramienta para introducirse en la mente de casi cualquier persona del mundo. Habían jaqueado el sistema político; habían hallado el modo de recopilar y analizar tantos datos sensibles que podían construir las campañas políticas más personalizadas de la historia... con las consecuencias desastrosas que ya conocemos.

En cuanto los científicos de datos de Cambridge Analytica tenían todos los datos que lograban reunir sobre ti, lo primero que hacían era clasificarte en una categoría muy concreta de personalidad. Te puntuaban conforme a los llamados «cinco grandes» rasgos de la personalidad, es decir, según tu grado de apertura a nuevas experiencias, tu preferencia por la planificación frente a la espontaneidad, tu grado de extroversión o introversión, tu nivel de afabilidad y tu propensión a experimentar emociones negativas como la ira y el miedo.

El segundo paso consistía en aplicar sus algoritmos predictivos al perfil que de ti hubieran trazado y calcular —sobre una escala del 0 al 100 por ciento— cuál era la probabilidad de que fueras a votar, por ejemplo, o de que te implicaras políticamente a propósito de algún tema.

El tercer paso era saber dónde pasabas el rato para que pudieran llegar hasta ti. ¿Veías mucho la televisión? ¿YouTube? ¿Había alguna plataforma de las redes sociales a la que dedicaras una cantidad de tiempo mayor? Cambridge Analytica te mostraba entonces contenido diseñado de forma específica para personas como tú y comprobaba si este surtía algún efecto en ti. ¿Te interesabas por ese contenido o no? En caso negativo, lo afinaban y probaban de nuevo. [55]

Los científicos de datos de Cambridge Analytica estudiaban cuál era la satisfacción vital de las personas. Siguiendo la lógica de los jáqueres, buscaban grietas y puntos débiles en nuestras mentes. Identificaban a las personas más influenciables, como, por ejemplo, las más propensas a sospechar de otros. Seleccionaban aquellas que manifestaban los rasgos característicos de la llamada «tríada oscura» (el narcisismo, el maquiavelismo —consistente en una priorización despiadada del interés propio— y la psicopatía) y las convertían en blanco de sus acciones con el objetivo expreso de suscitar su ira. Encendían los ánimos de los troles. Mostraban a las personas seleccionadas blogs que

ridiculizaban a individuos como ellas para hacer que se sintieran atacadas. Creaban páginas falsas en las redes sociales y llegaban incluso a organizar reuniones presenciales a las que acudían miembros del personal de Cambridge Analytica de incógnito. [56]

Al menos dos elementos hacían que las campañas digitales de Cambridge Analytica fueran especialmente peligrosas. En primer lugar, mostraban contenidos radicalmente diferentes a personas distintas, con lo que destruían el carácter compartido de la experiencia colectiva. El contenido que se comentaba y se analizaba en los medios convencionales no era como el que los votantes veían en línea. Las personas sometidas a herramientas diseñadas para confundir no pueden debatir entre ellas de un modo racional sobre un candidato en particular porque no están accediendo a la misma información. Sencillamente, era imposible que dos personas hablaran con serenidad sobre las luces y las sombras de una candidata como Hillary Clinton si una de ellas creía que esta estaba vinculada con una red de sexo infantil dirigida desde una pizzería en Washington, por ejemplo.

Un segundo elemento que hacía de Cambridge Analytica algo peligroso era que sus campañas no parecían tales. No tenían aspecto de propaganda cuidadosamente diseñada. A veces parecían información periodística. En otras ocasiones, presentaban la apariencia de unos contenidos creados por usuarios corrientes. Nadie sabía que lo que parecían movimientos sociales de base eran, en realidad, unas campañas políticas orquestadas por mercenarios digitales (y las más ignorantes de este hecho eran las personas que se veían arrastradas por aquellas polarizadas —y polarizadoras— opiniones).

Channel 4 emitió el resultado de una impactante investigación periodística con cámara oculta en la que a Mark Turnbull, el entonces director gerente de Cambridge Analytica, se le oía decir: «Nosotros solo inyectamos información en el torrente sanguíneo de internet [...] y observamos cómo crece, le vamos dando algún que otro empujoncito..., como por control remoto. Tiene que ocurrir sin que nadie piense “Esto es propaganda”, porque en cuanto alguien piensa eso [...], la siguiente pregunta es “¿Quién ha puesto eso ahí?”». [57]

El repertorio de iniciativas de guerra psicológica y de información empleado por Cambridge Analytica era extenso y no conocía límites morales. Incluía bulos personalizados, campañas de alarmismo (hasta el punto de mostrar escenas sangrientas de torturas y asesinatos reales), suplantaciones de identidad y toda una serie de servicios muy poco éticos, como «trampas para atrapar a rivales con proposiciones turbias (de soborno, sexo, drogas, etcétera), campañas de desmotivación del electorado, obtención de información para desacreditar a oponentes políticos y difusión anónima de información en plena campaña

electoral». [58] Esta fue la empresa que ayudó a Trump a ganar la presidencia de Estados Unidos y que también colaboró con los partidarios de Leave en la campaña del referéndum del Brexit (aunque a través de una firma política asociada, AggregateIQ [AIQ]); es, además, una compañía que, al parecer, guarda una estrecha relación con Rusia. [59] Espero que llegue un día en que quienes vengan después de nosotros lean lo que sucedió en este vergonzoso episodio de la historia y les cueste creerlo porque se sientan seguros al saber que sus democracias son sólidas y están lo bastante bien reguladas como para que nadie pueda volver a salirse con la suya intentando algo parecido.

Cambridge Analytica cerró, pero muchas de las personas que constituyeron la empresa han fundado luego nuevas compañías especializadas en datos. [60] AggregateIQ, la firma política canadiense implicada en el referéndum del Brexit que, según el denunciante Christopher Wylie y según las pruebas citadas por la Oficina del Comisionado de Información de Reino Unido, tenía un estrecho vínculo con SCL (la sociedad matriz de Cambridge Analytica), [61] sigue funcionando. Cambridge Analytica solo es un ejemplo de algo que cualquiera con conocimientos de análisis de datos puede hacer. En 2018, Tactical Tech, una ONG con sede en Berlín, tenía identificadas a más de 300 organizaciones en todo el mundo que colaboraban con partidos políticos orquestándoles campañas basadas en datos. [62] Rusia es bien conocida por sus intentos de inmiscuirse en la política interior de otros países para sembrar discordia entre conciudadanos valiéndose de perversos mecanismos de interferencia en los entornos digitales. En 2016, dos páginas de Facebook controladas por troles rusos organizaron una manifestación y una contramanifestación en Texas. La manifestación inicial, «Paremos la islamización de Texas», fue orquestada por un grupo de Facebook con más de 250.000 seguidores, llamado Corazón Texano y gestionado por una fábrica de troles, la Internet Research Agency, desde Rusia. La contramanifestación fue organizada de modo parecido por un grupo de Facebook controlado desde ese mismo país, United Muslims of America, que tenía más de 300.000 seguidores. [63] Como bien ilustra este caso, aunque Cambridge Analytica haya desaparecido, nuestras democracias todavía corren peligro.

El poder de Cambridge Analytica procedía de nuestros datos. El poder de otros actores maliciosos también deriva en parte de nuestros datos. El poder de las grandes tecnológicas viene de nuestros datos: de ese divertido cuestionario sobre personalidad que respondiste en línea para ver a qué personaje de dibujos animados te pareces más (esos cuestionarios están diseñados con la única finalidad de recopilar datos sobre ti), de aquella aplicación sospechosa que te descargaste un día y te pidió acceso a tus contactos, de esas «tarjetas cliente» que llevas en la cartera.

Los científicos de datos están jugando con nuestras vidas como si fueran unos dioses bebés que van por ahí agarrando cualquier cosa que ven como si fuera suya. Se han movido rápido y han roto cosas: vidas, nuestra capacidad de centrarnos en una sola cosa a la vez, y hasta democracias. Mientras tengan acceso a nuestros datos, seguiremos siendo sus títeres. La única manera de volver a tomar el control de nuestra autonomía, de nuestra capacidad de autogobernarnos, es recuperando nuestra privacidad.

PRIVACIDAD, AUTONOMÍA Y LIBERTAD

La autonomía es la capacidad y el derecho de gobernarte a ti mismo. Como ser humano adulto, eres capaz de decidir cuáles son tus valores —qué es significativo para ti, qué clase de vida quieres llevar— y de actuar de acuerdo con esos valores. [64] Cuando tomas una decisión autónoma, eres plenamente dueño de esta. Es la clase de decisión que expresa tus convicciones más profundas, una elección que puedes seguir suscribiendo después de haber reflexionado sobre ella.

Los individuos tienen un gran interés en que se respete su autonomía. Queremos que otros reconozcan y respeten nuestra capacidad de vivir nuestras vidas como nos parezca oportuno. En las democracias liberales, con muy pocas excepciones, nadie —ni siquiera el Estado— puede decirte qué pensar, qué decir, qué hacer para ganarte la vida, con quién relacionarte, ni cómo pasar el tiempo. Tú decides todas esas cosas y más. Sin autonomía, no tienes libertad, porque tu vida está controlada por otros. *Tener autonomía significa tener poder sobre tu propia vida* .

La autonomía es tan importante para el bienestar individual y social que cualquier interferencia con ella tiene que tener una justificación muy sólida; por ejemplo, la de evitar un daño a otras personas. Inmiscuirse en la autonomía de las personas para aumentar tus ganancias económicas, por ejemplo, no es justificable.

La privacidad y la autonomía están relacionadas porque las pérdidas de privacidad facilitan la intromisión de terceros en tu vida. Ser observados todo el tiempo interfiere en la tranquilidad que se necesita para tomar decisiones autónomas. Cuando el legendario bailarín Rudolf Nuréyev decidió desertar de la Unión Soviética durante una visita a Francia en 1961, las autoridades galas lo obligaron (por ley) a que permaneciera a solas cinco minutos en una sala antes de firmar una solicitud de «estatus de refugiado político» a fin de protegerlo de las autoridades rusas que estaban tratando de obstaculizar su decisión. [65] Una

persona necesita tiempo y espacio libres de presiones externas para decidirse sobre qué quiere para sí misma, y para disponer de la libertad para llevar a cabo lo que desea. Piensa, por ejemplo, en cómo las cabinas de votación se han diseñado para proteger al votante de presiones externas; si nadie puede ver a quién votas, nadie puede obligarte a votar en contra de tus deseos.

Cuando las personas saben que las están observando, y que cualquier cosa que hagan puede tener consecuencias negativas para ellas, tienden a autocensurarse. Cuando tú no buscas información sobre un concepto por miedo a que otros puedan utilizar esa información sobre ti, tu autonomía y tu libertad se ven coartadas. Tras las revelaciones de Edward Snowden sobre el alcance de la vigilancia de Estado, las búsquedas en Wikipedia relacionadas con el terrorismo se desplomaron en casi un 30 por ciento, ejemplificando el llamado «efecto inhibitorio» que tiene la vigilancia. [66]

Que otros usen tu información personal para manipular tus deseos es también una forma de que interfieran en tu autonomía, sobre todo cuando su influencia es encubierta. [67] Si no caes en la cuenta de que el contenido al que estás accediendo en línea es más un reflejo de lo que los anunciantes o los científicos de datos creen que eres que una representación del mundo exterior, será más difícil que actúes de modo racional y conforme a tus propios valores. Para tener autonomía, es necesario estar relativamente bien informado sobre el contexto en el que vives. Cuando otros manipulan tus ideas sobre el mundo y te inducen a creer en una falsedad que influye en cómo te sientes y cómo vives, están obstaculizando tu autonomía.

Las compañías tecnológicas tienen un largo historial de despreocupación total por nuestra autonomía. Muchas de esas empresas no parecen estar muy interesadas en lo que *nosotros* queremos. No fabrican productos para ayudarnos a vivir la vida que queremos vivir, ni para ayudarnos a convertirnos en las personas que queremos ser. Hacen productos que las ayuden a ellas a conseguir *sus* objetivos, productos que nos exprimen todos los datos posibles en su beneficio. Crean apps que nos vuelven adictos a las pantallas. Nos hacen firmar términos y condiciones en los que nos informan de los pocos (o nulos) derechos que nos asisten frente a ellas. Muchas compañías estarían encantadas de reducir aún más nuestra libertad. Este desprecio corporativo por la autonomía constituye una nueva forma de autoritarismo blando.

No es ninguna exageración afirmar que a Google le gustaría tener poderes divinos. Para empezar, quiere ser omnisciente: se esfuerza al máximo por recopilar todos los datos posibles para saberlo todo. En segundo lugar, quiere ser omnipresente: se propone ser la plataforma a través de la que nos comuniquemos con otras personas, veamos contenidos digitales, busquemos en línea, nos

orientemos por las calles de una ciudad o accedamos a la sanidad, entre otras cosas (en parte, porque así puede recabar más datos). En tercer lugar, quiere ser omnipotente: le gustaría tener la capacidad de llevarse lo que desee (o sea, nuestros datos) según sus propias condiciones y transformar el mundo a su favor. A tal efecto, gasta en cabildeo e influencia política más dinero que ninguna otra empresa estadounidense. [68]

Eric Schmidt dejó muy claro que a Google le gustaría hacerse con el control de nuestra autonomía: «El objetivo es permitir que los usuarios de Google puedan preguntar [...] cosas como "¿Qué haré mañana?" o "¿Con qué trabajo me quedaré?"». [69] En 2010, llegó más lejos todavía: «En realidad creo que la mayoría de la gente no quiere que Google responda a sus preguntas. Lo que quiere es que Google les diga qué deberían hacer a continuación». [70]

Puede que Google trate de convencerte de que sus recomendaciones se basan en tus valores porque te conoce muy bien. Sin embargo, no debemos olvidar que empresas como Google tienen un conflicto de intereses, porque lo que es mejor para ti (y para la sociedad en general) probablemente no sea lo mejor para su negocio. Este desalineamiento de intereses, sumado al nefasto historial de mala conducta de las compañías tecnológicas, nos proporciona motivos de sobra para negarnos a confiarles nuestra autonomía. Pero incluso si compañías como Google fuesen más de fiar, tu autonomía es demasiado importante como para delegarla a cualquiera que no seas tú.

Tal vez pienses que no hay de qué preocuparse, porque siempre puedes no hacer caso de las recomendaciones de Google. Si Google Maps te dice que vayas por un determinado camino, siempre puedes ignorarlo y seguir una ruta diferente. Sin embargo, no debemos subestimar la influencia que la tecnología ejerce sobre nosotros. Las tecnológicas no solo diseñan sus productos, sino que también nos diseñan a nosotros, los usuarios, al influir en nuestro comportamiento. Como dijo Winston Churchill: «Nosotros damos forma a nuestros edificios, y luego nuestros edificios nos dan forma a nosotros».

Una de las razones por las que a las compañías tecnológicas se les está dando tan bien predecir nuestra conducta es porque la están forjando en parte. Si una empresa posee el control de una parte importante de tu vida a través de tu teléfono inteligente y tu ordenador, e influye en ella eligiendo el contenido al que puedes acceder, y controlando las plataformas que utilizas para conectarte con otros, para comprar y para trabajar, no le va a costar mucho prever lo que harás a continuación; a fin de cuentas, es ella la que te proporciona las opciones y la que te va induciendo a una cosa o a otra. Está creando un entorno controlado para ti, como si de *El show de Truman* se tratara (si no has visto la película, te la recomiendo).

Que tu autonomía esté siendo amenazada por la tecnología es algo que debería preocuparte. Deberías ser dueño de tu propia vida. Y también es motivo de preocupación para el resto de nosotros. Aun si tú disfrutases de plena autonomía, seguirías teniendo muy buenos motivos para querer que los demás miembros de tu sociedad disfruten de ella también. El autogobierno de una comunidad política depende de que los individuos sean autónomos; si la autonomía individual disminuye, también lo hace el autogobierno colectivo. Para que una democracia sea una democracia, sus ciudadanos tienen que tener poder sobre sus propias vidas.

Una democracia en la que las personas no son autónomas es una farsa. Cuando los individuos tienen una autonomía débil, es fácil influir en ellos para que voten en un sentido que no refleja sus convicciones más profundas, sino más bien la capacidad de los poderosos para manipular percepciones y creencias.

Necesitamos que protejas tu privacidad para que podamos recuperar nuestra autonomía y nuestra libertad como sociedad. Aunque no te preocupen demasiado tus propios datos personales, nosotros —tu familia y amigos, tus conciudadanos, tus congéneres humanos alrededor del mundo— necesitamos que los tengas a buen recaudo, porque la privacidad es una empresa colectiva.

LA PRIVACIDAD ES COLECTIVA

La privacidad no es solo cosa tuya. Cuando se dice que tus datos son «personales» parece que se esté dando a entender que tú eres la única parte interesada a la hora de compartirlos. Pero ese es un error de concepto. La privacidad es tan colectiva como personal. [71] Como el desastre de Cambridge Analytica ha demostrado, cuando expones privacidad, nos pones a todos en peligro.

La privacidad se asemeja en ese sentido a los problemas ecológicos y de acción colectiva en general. Por mucho que te esfuerces en minimizar tu huella ecológica, si otros no ponen de su parte, todos sufriremos las consecuencias del calentamiento global. Estamos juntos en esto y necesitamos que suficientes personas remen en la misma dirección para que las cosas cambien.

El carácter colectivo de la privacidad tiene implicaciones profundas en cuanto a nuestra concepción de los llamados «datos personales». Se ha puesto de moda argumentar que estos deberían tratarse como una propiedad y que, por lo tanto, tendríamos que permitir que las personas vendieran o comerciaran con sus propios datos. Ahora proliferan las empresas que te permiten ser bróker de tu propia información. Como las sociedades capitalistas son muy respetuosas de la

propiedad privada, nos resulta intuitivo pensar que, dando a los datos personales el trato deferente que otorgamos a la propiedad, seremos respetuosos también con la privacidad. Sin embargo, no es así. [72]

Imaginemos que un amigo (o quizá un enemigo) te regala un kit doméstico de análisis de ADN. Se venden por unas 100 libras (unos 116 euros). Si envías una muestra de tu saliva, estarás cediendo la mayoría (o la totalidad) de tus derechos sobre tu información genética. [73] Eso significa que compañías como Ancestry pueden analizar, vender y comunicar esa información como les plazca. Carecer de privacidad genética puede ser negativo para ti. Son muchos los tipos de seguro que te obligan a comunicar los resultados de las pruebas genéticas que te hayas realizado, y esa información puede provocar que te denieguen la cobertura solicitada o que tengas que pagar primas más altas. Si no revelas los resultados de tu prueba y la aseguradora se entera de que los has ocultado (algo muy probable, dado que la mayoría de las empresas de análisis de ADN venden esos datos para sostener su negocio), esta puede rescindir tus pólizas. [74]

Quizá estés dispuesto a asumir esos riesgos a título individual. Puede que sientas curiosidad por saber si tienes un gen que te hace estornudar cuando tomas el sol (es uno de los elementos incluidos en los informes de 23andMe), [75] o tal vez tengas razones más serias para querer saber más sobre tu genética personal. Pero ¿y tu familia? Tus padres, hermanos e hijos tal vez no se alegren demasiado de verse privados de su privacidad genética. [76] No hay forma de saber cómo evolucionará la ley de aquí a dos o tres décadas, ni de conocer de antemano lo que entonces seremos capaces de inferir a partir de la información genética. A tus nietos se les pueden negar oportunidades en el futuro basándose en esa prueba genética que te realizaste, y eso sin que ellos consintieran en ningún momento que tú donaras o vendieras esos datos sobre sus genes.

Aunque tu ADN te hace ser quien eres, compartes la mayoría de tu composición genética con otras personas, incluso con parientes muy lejanos. La proporción de genes que son específicamente tuyos es en torno al 0,1 por ciento. Piénsalo de este modo: con una versión impresa de tus genes se llenarían unas 262.000 páginas, pero solo entre 250 y 500 de estas serían únicamente tuyas. [77]

Puesto que las similitudes y las diferencias entre nuestros genes permiten efectuar inferencias, no hay modo alguno de pronosticar qué uso se podría llegar a hacer de tu ADN. En el mejor de los casos, ese ADN podría ayudar a atrapar a un delincuente peligroso. Así fue como consiguieron detener al llamado Asesino del Golden State, homicida y violador en serie, en California en 2018. La policía subió a GEDmatch (una base de datos gratuita en línea en la que se almacenan resultados de pruebas genéticas de uso comercial) el ADN que había tomado del

escenario de uno de sus crímenes. La consulta reveló la existencia en aquella base del rastro genético de unos primos terceros del delincuente, cuyas identidades condujeron luego a las autoridades hasta el sospechoso. [78]

Quizá te parezca que esas son buenas noticias. Nadie en su sano juicio quiere que haya asesinos en serie sueltos por ahí. Sin embargo, no deberíamos dejar que una tecnología campe descontrolada ateniéndonos únicamente a cuál sea el mejor uso que se le pueda dar. Las tecnologías pueden utilizarse de muchos modos y las buenas prácticas rara vez son las únicas. Las bases de datos genéticos pueden emplearse para identificar a disidentes políticos, denunciantes y manifestantes antigubernamentales en países autoritarios. Incluso en regímenes democráticos se puede recurrir a las bases de datos de uso comercial para inferir la nacionalidad de los migrantes y deportarlos. [79]

Combinando una muestra anónima de ADN de una persona con alguna información adicional —por ejemplo, su edad aproximada—, se puede seleccionar por descarte una lista de menos de una veintena de candidatos entre los que identificarla partiendo de una base de datos de un millón trescientas mil personas. En 2018, una búsqueda así podía permitir la identificación de un 60 por ciento de los estadounidenses blancos, aunque muchos nunca hubieran proporcionado su propio ADN a una base de datos de genealogía familiar. [80] Cuantas más personas sigan facilitando su información genética, más factible resultará identificar a cualquier individuo en el mundo. Eso asumiendo que todo funcione como se supone que lo debe hacer, porque, a veces, no es así.

Las pruebas genéticas pueden comportar un alto índice de falsos positivos. Una cosa es usar el ADN como prueba de cargo contra alguien a quien ya se considere sospechoso por algún otro indicio, y otra, muy distinta, es ir por ahí realizando expediciones genéticas en busca de posibles sospechosos; esto último es peligroso. El ADN nos puede parecer una prueba irrefutable. La intuición nos invita a pensar que, si se encuentra la huella genética de una persona en el escenario de un delito, esa persona tiene que ser culpable. Pero no es tan sencillo. Son muchas las vías por las que el ADN puede acabar en una investigación penal. Cuando se estaba buscando a un delincuente apodado el Fantasma de Heilbronn, se encontró el ADN de un individuo en más de cuarenta escenarios de delitos en Europa. El ADN en cuestión resultó ser el de un operario industrial que fabricaba los bastoncillos usados por la policía para recoger muestras. Es muy fácil que se produzcan casos de contaminación genética. Otras veces los resultados de un análisis de ADN pueden intercambiarse por accidente con los de otra persona. Y, en la mayoría de las ocasiones, los datos genéticos son difíciles de interpretar. La búsqueda de similitudes entre dos muestras genéticas distintas implica una interpretación

subjetiva. Los errores son muy comunes. [81]

Tú puedes ser del todo inocente de un delito y, aun así, convertirte en sospechoso por culpa del análisis de ADN que se hizo un pariente tuyo. Así fue como Michael Usry adquirió la condición de sospechoso de asesinato. [82] Su padre había donado su ADN a un proyecto genealógico. Al final, y por suerte para Usry, se comprobó que, si bien el ADN de su padre era similar al hallado en el lugar de los hechos, el suyo particular no lo era. Tras una espera de treinta y tres días que debieron de hacérsele eternos, Usry fue descartado como sospechoso. No todo el mundo es tan afortunado. Son muchos los casos de personas a quienes se ha condenado por error basándose en una prueba de ADN. [83] Según el Registro Nacional de Exoneraciones de Estados Unidos, las pruebas forenses falsas o engañosas fueron un factor en el 24 por ciento de todas las condenas que se han podido demostrar erróneas en aquel país. [84] Y esos solo son los casos conocidos.

Del mismo modo que todos estamos relacionados por nuestra composición genética, también estamos ligados unos a otros por un sinfín de hilos invisibles que hacen que seamos vulnerables a los deslices de privacidad cometidos por otras personas. Si publicas información acerca de dónde vives, estás exponiendo a las personas con las que compartes domicilio y a tus vecinos. Si das a una empresa acceso a tu teléfono, estás exponiendo a tus contactos. Si divulgas información sobre tu psicología, estás exponiendo a otras personas que comparten esos mismos rasgos psicológicos. Puede que tú y yo no nos hayamos conocido nunca y puede que jamás coincidamos en el futuro, pero, aun así, si tenemos suficientes rasgos psicológicos en común y tú cedes tus datos a organizaciones como Cambridge Analytica, también les estás cediendo parte de mi privacidad. Puesto que estamos interrelacionados por vías que nos hacen mutuamente vulnerables, cada uno es en parte responsable de la privacidad de los demás.

Nuestra interdependencia en materia de privacidad implica que ningún individuo cuenta con la autoridad moral para vender sus datos. No somos dueños de nuestros datos personales como lo somos de una propiedad, porque nuestros datos personales contienen los de otros individuos. Tus datos personales no son solo tuyos.

La privacidad es colectiva en al menos dos sentidos. Lo es no solo porque esos deslices por los que revelas tus asuntos privados pueden facilitar violaciones del derecho a la privacidad de otras personas, sino también porque las consecuencias de las pérdidas de privacidad se sufren a escala colectiva. La cultura de la exhibición de lo privado perjudica a la sociedad. Daña el tejido social, supone un riesgo para la seguridad nacional (como veremos más

adelante), permite la discriminación y pone en peligro la democracia.

Vivir en una cultura en la que todo lo que haces o dices puede difundirse a millones de individuos somete a las personas a una presión considerable. Sentir que nunca podemos cometer un error en público cuando nuestros espacios privados se han estrechado tanto es una carga enorme sobre nuestras espaldas. Casi todo lo que hacemos es potencialmente público. Los seres humanos no podemos desarrollarnos si vivimos permanentemente expuestos en un escaparate. Cuando confiamos en que otros no divulgarán lo que decimos, es más fácil que seamos sinceros, audaces e innovadores.

No hay intimidad sin privacidad. Las relaciones que no pueden confiar en un escudo de confidencialidad —bien porque desconfiamos de otros, bien porque no nos fiamos de las tecnologías que usamos para comunicarnos e interactuar con otros— están condenadas a ser más superficiales. Es necesario que impere cierta cultura de la confidencia para disfrutar de conversaciones íntimas con otras personas, mantener debates francos dentro de entornos cerrados como los domicilios o las aulas y afianzar los lazos sobre los que se fundamentan las sociedades liberales. Estar en un mundo en el que los datos se usan continuamente como armas es sentirte permanentemente amenazado y receloso de los demás. Ese miedo genera conformidad y silencio.

Cuando imparto una clase o doy una conferencia en un contexto en el que todo se está grabando (o, peor aún, transmitiéndose en directo en línea por *streaming*), suelo notar que me reprimo en algunas de las cosas que digo y que mis alumnos o el público asistente formulan preguntas menos polémicas. Me han dicho que, desde que los juicios comenzaron a grabarse en España, se han extendido los momentos de silencio. [85]

La «espiral del silencio» es la tendencia que tienen las personas a no expresar sus opiniones en público cuando creen que estas no son lo bastante compartidas por otros. Las investigaciones al respecto dan a entender que tanto las redes sociales como la vigilancia en general provocan una acentuación de esa espiral del silencio. [86] El miedo a sufrir aislamiento social y otras repercusiones negativas empuja a las personas a conformarse. Cuando la vigilancia está en todas partes, es más seguro quedarse callado o hacerse eco de las opiniones aceptadas por otros. Pero la sociedad solo progresa a través de escuchar los argumentos de los críticos, de aquellos que se rebelan contra el *statu quo* .

La ausencia de privacidad también daña a la sociedad cuando se usan datos personales con el propósito de adaptar los bulos y la propaganda a cada individuo. Cuando unos actores maliciosos difunden *fake news* personalizadas, a veces lo hacen con un objetivo muy concreto en mente, como, por ejemplo, el de ayudar a un candidato específico a vencer en una contienda electoral. Sin

embargo, a menudo, su objetivo último no es otro que sembrar discordia en la sociedad. La de «divide y vencerás» es una estrategia política muy antigua que se ha modernizado con las redes sociales. Se nos divide en función de nuestros datos personales y se nos vence a través de la propaganda personalizada.

Todo el mundo es vulnerable a la manipulación porque nadie tiene un acceso sin intermediarios a la información. Es imposible que seas testigo de primera mano de todo lo relevante que ocurre en tu país y en el mundo. Te informas sobre los candidatos y sobre la actualidad política a través (sobre todo) de tus pantallas. A menudo, ni siquiera escoges tus fuentes. No eres tú quien va a buscarlas, sino que ellas te buscan a ti. Aparecen en las «noticias» que Twitter o Facebook te envían a través de sus *feeds* . Y, aunque parezca que lo hacen como por arte de magia o por casualidad, las empresas como Facebook ponen mucho de su parte en gestionar esos contenidos. Se especializan en vender tu atención a actores desconocidos que quieren influenciarte.

Si tú y yo recibimos información contradictoria sobre un candidato y ninguno de los dos podemos ver lo que el otro ha visto, es probable que, cuando hablemos del político en cuestión, cada uno termine pensando que el otro es un estúpido, un loco o ambas cosas, sin darnos cuenta de que estamos experimentando la realidad a través de unos filtros muy diferentes. Filtros que además han sido colocados específicamente para cada uno de nosotros por alguien que quiere que nos odiemos. Cuando no podemos ver una misma realidad, la sociedad se polariza y los malos ganan. Las sociedades polarizadas son más frágiles. La cooperación se hace difícil y resolver problemas que requieren de una acción colectiva se vuelve imposible. Cuando cada uno de nosotros está atrapado en una especie de cámara de resonancia aislada, o en un gueto informativo, no hay forma de interactuar de un modo constructivo.

Otra manera que los actores maliciosos tienen de sembrar discordia en línea es fomentando emociones negativas en la población. Cuanto más asustados y enojados estemos, más desconfiamos los unos de los otros, menos racionales son nuestras decisiones y peor funcionan nuestras sociedades.

El poder que la privacidad nos confiere de manera colectiva, como ciudadanos, es necesario para la democracia: para que votemos conforme a nuestras creencias y sin presiones indebidas, para que podamos protestar de forma anónima sin miedo a represalias, para que ejerzamos nuestra libertad de asociación, para que digamos lo que pensamos, para que leamos aquello que nos produce curiosidad. Si vamos a vivir en democracia, el grueso del poder tiene que residir en la ciudadanía. Y quien tenga los datos tendrá el poder. Si la mayor parte del poder reside en las empresas, viviremos en una plutocracia, una sociedad gobernada por los ricos. Si la mayoría del poder reside en el Estado,

tendremos una forma u otra de autoritarismo. Para que el poder de los Estados sea legítimo, tiene que provenir del consentimiento de la ciudadanía —no de nuestros datos. La democracia liberal no es algo que se pueda dar por hecho. Es algo por lo que tenemos que luchar a diario. Y, si dejamos de construir las condiciones que permitan su desarrollo, la democracia liberal desaparecerá. La privacidad es importante porque da poder a la ciudadanía. La privacidad es un bien público y defenderla es nuestro deber cívico. [87]

¿POR QUÉ LA DEMOCRACIA LIBERAL?

La «democracia» es un sistema de gobierno en el que el poder soberano reside en el pueblo. La democracia aspira a que una sociedad de iguales se gobierne a sí misma y logre establecer un orden social relativamente justo sin dictadores ni mandatarios autocráticos. [88] Hace unas décadas, para defender la privacidad tal vez habría bastado con decir que esta es necesaria para sostener las democracias liberales. Hoy, sin embargo, la democracia no está en el punto más alto de su popularidad. Solo un tercio de los estadounidenses menores de treinta y cinco años atribuye una importancia vital al hecho de vivir en una democracia, y el porcentaje de quienes acogerían de buen grado la llegada de un régimen autoritario militar ha aumentado desde el 7 por ciento en 1995 hasta un 18 por ciento en 2017. [89] Alrededor del mundo, los derechos civiles y políticos han experimentado un declive en los últimos doce años: en 2017, solo treinta y cinco países habían mejorado, mientras que setenta y uno habían empeorado. [90] The Economist Intelligence Unit calificó 2019 como «un año de reveses democráticos» en el que la puntuación media de la democracia en el mundo alcanzó su nivel más bajo desde 2006 (año en el que comenzó a elaborarse el Índice de Democracia Global). [91] Los ataques contra la democracia se han acelerado aún más durante la pandemia de coronavirus. Según Freedom House, un *think tank* de Washington, la democracia y el respeto por los derechos humanos se han deteriorado en ochenta países desde el estallido inicial de la pandemia. [92]

Resulta necesario, pues, explicar por qué debes seguir luchando por la democracia liberal, aunque el presidente (o primer ministro) en ejercicio en tu país sea un imbécil. Aunque pienses que el Gobierno actual (o los anteriores, o todos ellos) han arruinado tu país. Aunque te sientas excluido del proceso político. Aunque no te sientas representado por tus políticos locales. Aunque sospeches que tu sociedad ha sido jaqueada. Aunque desconfíes de tus conciudadanos (*sobre todo* si desconfías de tus ciudadanos). Aunque la

democracia te haya decepcionado, deberías hacer un esfuerzo por mejorarla y no por librarte de ella, porque es el sistema que más adecuadamente protege los derechos fundamentales de todos, incluidos los tuyos.

«Nadie puede pretender que la democracia sea perfecta o completamente sabia —dijo Winston Churchill en una célebre alocución en 1947—. De hecho, se dice que la democracia es la peor forma de gobierno, a excepción de todas las demás que se han ido probando hasta la fecha.» [93]

La democracia no es un sistema maravilloso. En su mejor versión, es desordenada, lenta hasta la exasperación y resistente al cambio. Está tan hecha a trozos que recuerda a una colcha de retazos cosida por un chiquillo de cinco años. Requiere acuerdos y concesiones, con lo cual, la mayoría de las veces, nadie consigue exactamente lo que quiere y todos se quedan algo insatisfechos. En la peor de sus versiones, es un sistema del que se puede apropiar un puñado de ricos y poderosos para dictar sus propias normas a la sociedad con el fin de beneficiarse a expensas de todos los demás.

Podemos estar de acuerdo en que la democracia no es un paraíso terrenal. Sin embargo, sí presenta ciertas ventajas que ningún otro sistema político tiene. La democracia obliga a los políticos a tener en cuenta los intereses y opiniones de la mayoría de las personas en la sociedad. Los políticos dependen de nuestro apoyo para estar en el poder, lo que los fuerza a intentar tener más o menos contenta a la mayoría de la población. El que la democracia implique a muchas más personas que otras formas de gobierno aumenta la probabilidad de que las decisiones tomadas sean mejores, pues se pueden aprovechar muchas fuentes de información y puntos de vista. [94] Las democracias tienden a ser más prósperas. También suelen ser más pacíficas, tanto dentro de sus fronteras como en su relación con otros países (una idea expresada por la llamada «teoría de la paz democrática», una tradición que se remonta a Immanuel Kant). [95] El filósofo Karl Popper nos recordó en su día que las democracias son el mejor sistema para deshacerse de los malos gobiernos sin derramamientos de sangre, y también para poner en práctica reformas sin violencia. [96]

Aun así, en las democracias existen muchos de los males que se pueden encontrar en las sociedades autoritarias. Si buscas ejemplos de abusos de poder y de injusticias, lo más probable es que no te cueste mucho dar con ellos. Sin embargo, lo que marca la diferencia es la frecuencia de esos casos. Una diferencia cuantitativa se convierte en cualitativa. George Orwell escribió que el mejor activo de la democracia es «la relativa sensación de seguridad» de la que pueden disfrutar sus ciudadanos. Poder hablar de política con los amigos sin sentir miedo. Tener la tranquilidad de que nadie te va a castigar a menos que infrinjas la ley, y saber que «la ley está por encima del Estado». [97] Que yo

pueda escribir este libro —en abierto desafío a algunos de los agentes más poderosos de nuestra sociedad— sin miedo y que tú puedas leerlo es la prueba de que vivimos en unas sociedades libres. No hay que darlo por sentado.

Para que tus derechos en particular estén garantizados, la democracia tiene que ser liberal. De otro modo, nos arriesgamos a padecer lo que John Stuart Mill llamó «la tiranía de la mayoría». Una mayoría puede ser tan opresora de una minoría como un autócrata. El liberalismo aspira a permitir a los ciudadanos el máximo de libertad posible asegurándose al mismo tiempo de que se respetan los derechos de todos. El liberalismo impone solamente los límites necesarios para que cada uno de nosotros pueda perseguir su ideal de la vida buena sin interferir en la de los demás. Si eres un ciudadano corriente, vivir en una democracia liberal es tu mejor opción para disfrutar de la máxima autonomía. Las democracias liberales permiten que nos autogobernemos, como individuos y como sociedades.

Cuando se desatiende el elemento liberal, las democracias pueden destruirse mediante un desmantelamiento del sistema desde dentro. Las democracias no siempre mueren con un gran estruendo, sino que también pueden morir a manos de dirigentes elegidos democráticamente. Hitler en Alemania y Chávez en Venezuela son dos ejemplos. [98] El filósofo británico Jonathan Wolffsostiene que el primer paso para que el fascismo termine anulando la democracia es priorizar la voluntad de la mayoría sobre los derechos de las minorías. El segundo paso es cuestionar los medios por los que se expresa esa voluntad de la mayoría, socavando así los procesos electorales. [99] (En la era digital debemos estar atentos a las pretensiones de las compañías tecnológicas cuando nos dicen cosas como que tus dispositivos pueden interpretar tu voluntad y votar en tu lugar. El experto en inteligencia artificial (IA) César Hidalgo, por ejemplo, argumenta que, en el futuro, deberíamos tener unos avatares digitales que voten en nuestro nombre. [100] Mala idea.)

La democracia liberal limita el gobierno de la mayoría para garantizar que se protejan los derechos de la minoría. En una democracia liberal, no puedes ir a prisión si no has incumplido la ley, por mucho que la mayoría de tu sociedad esté dispuesta a votar a favor de que se vulneren tus derechos. Para eso existe el Estado de derecho.

LA PRIVACIDAD ES LA VENDA EN LOS OJOS DE LA JUSTICIA

Una de las grandes virtudes de la democracia liberal es su énfasis en la igualdad y la justicia. Nadie está por encima de la ley, todo el mundo tiene los mismos

derechos, todas las personas mayores de edad pueden votar y todas tienen la oportunidad de participar en la democracia por vías más activas, incluso las personas que terminan en el lado perdedor de una votación. Uno de los mayores defectos de la economía de los datos personales es lo mucho que está minando la igualdad. En la esencia misma de la economía de los datos está el que a cada uno se nos trate de forma diferente, en función de nuestros datos. Es porque se nos trata de manera distinta por lo que los algoritmos terminan siendo sexistas y racistas, como hemos visto. Es porque se nos trata de forma diferente en función de nuestros datos por lo que, sin saberlo, unas personas pagan precios distintos de los que pagan otras por el mismo producto. Es porque se nos trata de manera desigual por lo que unos individuos vemos contenidos diferentes de los que ven otros, lo que amplifica aún más nuestras diferencias: todo un círculo vicioso de alteridad y desigualdad. Sin importar quién seas, deberías tener el mismo acceso que otros tienen a la información y a las oportunidades. La justicia se representa a menudo personificada como una mujer con los ojos vendados, simbolizando la imparcialidad. La privacidad es lo que puede vendar los ojos del sistema para que se nos trate con igualdad e imparcialidad. La privacidad es la venda en los ojos de la justicia.

Corregir las asimetrías de poder

Las grandes tecnológicas y los titiriteros políticos han tenido mucho éxito manipulándonos porque hemos padecido una asimetría de conocimiento que ha llevado a una asimetría de poder. Hasta hace poco, sabíamos muy poco sobre el funcionamiento de las grandes tecnológicas y la propaganda política en el entorno digital. Sus tácticas eran invisibles para nosotros. Mientras tanto, ellas lo iban aprendiendo casi todo sobre nosotros. Tenemos que esforzarnos por reequilibrar la balanza a nuestro favor. Tenemos que saber más sobre ellas y procurar que ellas sepan menos sobre nosotros. Leer este libro es un paso en la dirección correcta; te ayudará a informarte del poder de las grandes tecnológicas y los gobiernos. Salvaguardar mejor nuestra privacidad es el paso siguiente. Si mantienes sus datos a buen recaudo, ellos sabrán menos de ti como persona y menos de nosotros como colectivo de ciudadanos.

Hay tres guardianes de la verdad, la justicia y la imparcialidad cuya independencia es imperioso defender por el bien de la salud de las democracias liberales: la prensa, los tribunales de justicia y el mundo académico. Una parte importante de la corrección de las asimetrías de poder en la era digital consiste en apoyar a esos guardianes. Como miembro de la comunidad universitaria, me

preocupa que cada vez sea mayor la proporción de investigación (sobre ética, incluso) financiada por las grandes compañías tecnológicas. Si estas empresas quieren financiar la investigación, que lo hagan a través de unos intermediarios que garanticen una separación entre los investigadores y la fuente de su financiación. Los intermediarios en cuestión pueden ser gobiernos, fundaciones independientes o universidades, pero siempre y cuando los fondos se donen de un modo que los despoje de toda atadura a su fuente. Si se corre el riesgo de que los fondos para investigación desaparezcan cada vez que los investigadores defiendan un argumento controvertido, la libertad académica se verá comprometida y la sociedad sufrirá un perjuicio por ello. Los investigadores no podrían ocuparse de lo que consideren que es más importante estudiar y tampoco podrían divulgar sus conclusiones. Ya me ha tocado ver a investigadores que evitan enfoques polémicos y eligen temas que saben que las grandes tecnológicas verán con buenos ojos. Si alguien aspira a que Google financie su trabajo, ¿tú crees que se va a atrever a cuestionar la ética de la publicidad digital? Del mismo modo que debemos extremar el ojo crítico con las investigaciones médicas subvencionadas por las grandes farmacéuticas, o con los estudios sobre nutrición sufragados por empresas de alimentación, deberíamos recelar también de las investigaciones financiadas por las grandes compañías tecnológicas.

Durante los últimos años, el periodismo independiente —con la inestimable ayuda de quienes se han atrevido a denunciar desde dentro las prácticas ilícitas de algunas organizaciones— se ha convertido en uno de los más acérrimos adversarios de la sociedad de la vigilancia. Edward Snowden denunció el funcionamiento de la vigilancia masiva y tuvimos noticia de todo ello gracias a Laura Poitras, Glenn Greenwald, Ewen MacAskill y el diario *The Guardian* , dirigido en aquel entonces por Alan Rusbridger. Carole Cadwalladr, de *The Observer* , desveló las operaciones de Cambridge Analytica y dio a Christopher Wylie un altavoz con el que hacer pública su denuncia.

Todas estas personas han tenido que soportar enormes presiones para informarnos. Snowden tuvo que buscar asilo político en Moscú y es posible que no pueda regresar jamás a Estados Unidos. El esposo de Greenwald fue retenido e interrogado durante nueve horas en el aeropuerto de Heathrow (además de confiscársele el ordenador) bajo la ley antiterrorista británica. Laura Poitras fue retenida e interrogada en diversos aeropuertos en reiteradas ocasiones. *The Guardian* , amenazado por un requerimiento judicial y bajo la vigilante mirada de las autoridades gubernamentales, fue obligado a destruir los discos duros que contenían los documentos filtrados por Snowden. En el momento de escribir estas líneas, Carole Cadwalladr se enfrenta a una demanda por difamación

presentada por el millonario Arron Banks, uno de los impulsores de la campaña del Brexit. Si no fuera por periodistas valientes, no estaríamos al tanto de las reglas conforme a las que vivimos en la actualidad. Lee y apoya el buen periodismo; forma parte integral del autoempoderamiento de los ciudadanos frente al poder de las grandes empresas y los estados.

Los bulos y la propaganda comparten algunos elementos con el ilusionismo. Los trucos de magia captan nuestra atención y nos inspiran asombro, aunque sepamos que son ilusiones. Gustav Kuhn, un antiguo mago convertido en profesor de psicología, ha descubierto que las ilusiones pueden ser tan cautivadoras —aun cuando, a cierto nivel, sepamos que estamos siendo objeto de un engaño— que un buen truco nos hará creer que estamos presenciando algo paranormal. Solo cuando nos explican cómo se hace el truco nos liberamos del encantamiento. [101] Del mismo modo, entender cómo se diseñan los contenidos personalizados y con qué fines podría quitarles parte de su poder —podría romper el hechizo.

Resistir al poder

Tal y como estos ejemplos de periodismo brillante y valiente demuestran, no todo son malas noticias. Se puede resistir y desafiar al poder. Tú también tienes poder, y el que tenemos como colectivo es aún mayor. Las instituciones han acaparado demasiado poder durante la era digital, pero podemos recuperar los datos en los que este se sustenta y podemos limitar la recolección de nuevos datos. El poder de las grandes compañías tecnológicas parece muy sólido, pero en realidad es un castillo de naipes que depende de nosotros. Las grandes tecnológicas no son nada sin nuestros datos. Bastaría una pequeña normativa reguladora, un poco de resistencia ciudadana, o unas pocas empresas que empiecen a ofrecer privacidad a modo de ventaja competitiva para que todo el edificio se derrumbe.

Nadie es más consciente de su vulnerabilidad que las propias compañías tecnológicas. Por eso se esfuerzan tanto por convencernos de que se preocupan por nuestra privacidad (a pesar de lo que sus abogados defienden ante los tribunales). Por eso se gastan millones en cabildeo. [102] Si estuvieran tan seguras del valor de sus productos para el bien de los usuarios y la sociedad, no necesitarían ejercer toda esa presión política. Las compañías tecnológicas han abusado de su poder y es hora de que les opongamos resistencia.

En la era digital, la oposición inspirada por el abuso de poder ha recibido el nombre de *techlash* . [103] Los abusos de poder nos recuerdan que este solo

puede tener una influencia positiva en la sociedad cuando está restringido. Por muy entusiasta de las nuevas tecnologías que seas, o por mucho que pienses que lo que las compañías tecnológicas y los gobiernos están haciendo con nuestros datos no tiene nada de malo, debería interesarte igualmente que el poder esté limitado, porque nunca se sabe quién lo ocupará en el futuro. Tu próximo primer ministro podría ser más autoritario que el actual; los próximos directores ejecutivos de las grandes compañías tecnológicas que vengan podrían no ser tan benévolos como sus predecesores.

No te rindas ante la economía de los datos sin plantarle batalla. No cometas el error de pensar que estás a salvo de los perjuicios relacionados con la falta de privacidad solo porque dé la casualidad de que seas joven, hombre, blanco, heterosexual y goces de buena salud. Tal vez pienses que, en ese caso, tus datos solo pueden jugar a tu favor y nunca en tu contra (suponiendo que hayas tenido suerte hasta el momento). Pero podrías no estar tan sano como crees y, desde luego, no vas a ser joven toda la vida. La democracia que das ahora por sentada podría mutar en un régimen autoritario que tal vez no favorezca a los que se parecen a ti. Si regalamos todo nuestro poder al capitalismo de la vigilancia porque pensamos que nuestros actuales dirigentes son benévolos, luego no podremos recuperarlo cuando la cosa se ponga fea, ya sea porque lleguen nuevos líderes o porque los actuales nos decepcionen. Como dijo el político británico decimonónico John Dalberg-Acton: «El poder corrompe, y el poder absoluto corrompe de forma absoluta». No es prudente dejar que las compañías tecnológicas o los gobiernos tengan un poder excesivo sobre nosotros.

Antes de entrar en detalles sobre *cómo* volver a tomar el control de nuestros datos personales —y, con él, el de nuestra autonomía y nuestras democracias—, hay una razón más por la que deberíamos resistir la economía de los datos. Además de que crea desequilibrios de poder, la economía de la vigilancia es peligrosa porque comercia con datos personales, y los datos personales son una sustancia tóxica.

4

Datos tóxicos

El amianto es un material maravilloso en muchos sentidos. Es un mineral que puede extraerse del subsuelo con un bajo coste y presenta una durabilidad y una resistencia al fuego excepcionales. Por desgracia, además de muy práctico, el amianto también es mortal. Provoca cáncer y otras enfermedades pulmonares graves y no existe ningún umbral de exposición segura a este. [1] Los datos personales son el amianto de la sociedad tecnológica. Como el amianto, los datos personales pueden extraerse de forma barata. Buena parte de ellos son el subproducto de la interacción de las personas con las tecnologías. Son útiles, igual que el amianto. Se pueden vender, se pueden intercambiar por ventajas y pueden ayudar a predecir el futuro. Y, como el amianto, son tóxicos. Los datos personales pueden envenenar las vidas individuales, las instituciones y las sociedades.

El experto en seguridad Bruce Schneier sostiene que los datos son un activo tóxico. [2] Día tras día y semana tras semana, hay jáqueres colándose sin autorización en alguna red y robando datos sobre personas. A veces los usan para cometer algún fraude. Otras, los utilizan para humillar, extorsionar o coaccionar a alguien. Recopilar y guardar datos personales es una bomba de relojería, un desastre en potencia. En el ciberespacio, los atacantes tienden a partir con ventaja ante aquellos que se defienden. Mientras que el atacante puede elegir el momento y el método de su agresión, el defensor tiene que protegerse de cualquier tipo de asalto en todo momento. El resultado es que los atacantes tienen muchas probabilidades de hacerse con el acceso a esos datos personales si se lo proponen.

Los datos personales son peligrosos porque son un material sensible, muy susceptible de un mal uso, difícil de tener a buen recaudo y codiciado por muchos, desde delincuentes hasta empresas aseguradoras y agencias de inteligencia. Cuanto más tiempo tengan otros almacenados nuestros datos y cuanto más los analicen, más probable resultará que alguien acabe usándolos contra nosotros. Los datos son vulnerables y eso hace que, a su vez, los sujetos de datos y cualquiera que los guarde sean vulnerables también.

VIDAS INTOXICADAS

Si tus datos personales acaban en las manos equivocadas, pueden arruinarte la vida. No hay forma de prevenir el desastre y, una vez que ocurre, es demasiado tarde —los datos no se pueden retirar.

El 18 de agosto de 2015, más de 30 millones de personas se enteraron al levantarse por la mañana de que algunos de sus datos más personales aparecían revelados en línea. Unos jáqueres habían publicado íntegra la base de datos de clientes de Ashley Madison, un sitio de citas que ayuda a las personas casadas a tener aventuras extramatrimoniales. Sus usuarios (entre ellos, personas que ya se habían dado de baja como tales) figuraban allí con sus nombres, direcciones, preferencias, códigos postales y números de tarjeta de crédito. Los jáqueres querían dar una lección a quienes cometían infidelidades. «Reparad el daño», escribieron. [3]

Cuesta hacerse una idea exacta del rastro de sufrimiento y destrucción que aquella filtración de datos dejó tras de sí. Millones de personas tuvieron que soportar problemas de insomnio y ansiedad. Algunas perdieron su empleo. Otras fueron objeto de chantaje por parte de delincuentes que amenazaban con contárselo a sus cónyuges si no les pagaban para comprar su silencio. En un caso en concreto, la carta de extorsión contenía la siguiente amenaza: «Si no cumples con mi demanda, no solo voy a humillarte, sino que también voy a humillar a todos tus allegados». [4] Y, aunque la víctima pagara con la esperanza de que se preservara así el silencio, nunca podía estar segura de que ese mismo delincuente (u otro) no fuera a delatarla de todos modos. En Alabama, un periódico imprimió en sus páginas todos los nombres de las personas de la región que figuraban en la base de datos. Un jáquer, por pura diversión, abrió una cuenta de Twitter y un sitio web para publicar los detalles más salaces que pudo encontrar entre los datos filtrados. Se rompieron matrimonios y familias, y algunas personas se suicidaron. [5]

Tal vez pienses que los usuarios de Ashley Madison se lo tenían merecido por su infidelidad. Discutible. No está bien suponer que cualquiera que sea culpable de algo se convierte por ello en blanco legítimo del castigo social. Todos somos culpables de *algo* , al menos a ojos de algunos. Sin embargo, todo el mundo tiene derecho a la privacidad y, en nuestra sociedad, nadie ha otorgado a los jáqueres legitimidad moral alguna para juzgar y castigar a las personas. Además, la humillación en línea y la pérdida de un empleo no son castigos apropiados a una infidelidad. Y no olvidemos que algunos de los usuarios del sitio tenían razones complicadas para estar en él y no eran tan culpables como puede parecer a simple vista. Algunos estaban allí con el conocimiento y el consentimiento de

su pareja. Otros se habían apuntado porque sus cónyuges respectivos se negaban a dormir con ellos. Otros lo habían hecho en un momento de debilidad, pero nunca habían ido más allá de apuntarse: el inscribirse en el sitio solo había supuesto una especie de recordatorio de que podían buscar lazos con otras personas fuera de su matrimonio si lo deseaban. Y aun en el caso de que pienses que los usuarios de Ashley Madison se lo habían buscado, sus cónyuges e hijos eran inocentes y en ningún caso se merecían la humillación pública que tuvieron que soportar por asociación.

Tras leer sobre este desastre relacionado con los datos, tal vez des un suspiro de alivio y pienses que estás a salvo porque nunca has mentido a tu familia. (Tal vez tu familia te esté mintiendo a ti.) Pero no hace falta que tengas secretos turbios para que tus datos personales te intoxiquen la vida. Basta con algo tan banal como tu pasaporte, tu carnet de identidad, o tu nombre, tu domicilio y tus datos bancarios.

Dos hombres despertaron a Ramona María Faghiura en mitad de la noche en enero de 2015. Le mostraron una orden de detención y se la llevaron bajo arresto. Ella aseguró a los policías que no había hecho nada malo, pero de nada le sirvió. Intentó explicar que había sido víctima de un robo de identidad y que la persona a la que buscaban no era ella. Dio igual. Envió un mensaje de texto a su marido mientras iba sentada en la parte de atrás del furgón policial: «Estoy detenida. Tráete la carpeta». La carpeta en cuestión contenía un resumen de su pesadilla: documentos judiciales, citaciones, fianzas y todas sus denuncias ante los jueces y la policía, en las que se quejaba una y otra vez de que alguien se había valido de su identidad para cometer fraude en una docena de ciudades de España.

Ramona María Faghiura no había hecho nada malo. Sin embargo, se pasó años entrando y saliendo de comisarías y juzgados, y gastando miles de euros en abogados con la esperanza de que la ayudaran a demostrar su inocencia. Le diagnosticaron ansiedad y tuvo que medicarse. «Me está arruinando la vida», se lamentaba. [6]

Los casos de robos de identidad se han convertido en algo relativamente común en la era digital y los fraudes con tarjetas de crédito son su variante más habitual. Año tras año, vamos añadiendo más información en línea, creando más bases de datos públicas que los delincuentes pueden usar para inferir información sobre las personas, mientras nuestros protocolos de seguridad no están mejorando. No debería extrañarnos que los daños relacionados con los datos se estén convirtiendo en algo muy común. En una encuesta que mi colega Siân Brooke y yo realizamos hace poco, nada menos que un 92 por ciento de las personas consultadas dijeron haber sufrido algún tipo de violación de su

privacidad en línea, desde robos de identidad hasta humillaciones públicas y ataques con programas espía. [7]

Otro delito relacionado con los datos que está cada vez más extendido es la extorsión. En 2017, una banda criminal logró acceder a los datos de una clínica lituana de cirugía estética y chantajeó a los pacientes, procedentes de sesenta países de todo el mundo, exigiéndoles un rescate en bitcoins. Los jáqueres terminaron publicando más de 25.000 fotos privadas —incluidas algunas de desnudos— y datos personales como pasaportes escaneados y números de la seguridad social. [8]

Hace poco también han sido objeto de chantaje los pacientes de una clínica de psicoterapia de Finlandia a raíz de que un jáquer robara sus datos. Unos 300 historiales se publicaron en la web oscura. [9] En 2019, una mujer española, madre de dos niños pequeños, se suicidó después de que se compartiera un vídeo sexual suyo entre sus compañeros de trabajo en un grupo de WhatsApp. [10] Los rumores falsos difundidos a través de esa misma aplicación acerca del secuestro de niños han hecho que personas inocentes sufran palizas e incluso linchamientos en la India. [11] Un japonés acusado de acosar y agredir sexualmente a una mujer confesó a la policía que pudo dar con ella gracias a un reflejo que vio en sus ojos en una fotografía compartida a través de las redes sociales: distinguió en él una parada de autobús y utilizó Google Street View para localizarla. [12] En Estados Unidos, la policía de Detroit arrestó por error a un hombre basándose solamente en una correspondencia errónea obtenida a partir de un algoritmo de reconocimiento facial. [13] Los investigadores del caso creen que un teléfono jaqueado pudo haber sido lo que condujo a los asesinos del periodista Jamal Khashoggi hasta él para matarlo en Turquía en 2018. [14]

Estos son solo algunos ejemplos de las muchas formas en que las vidas de incontables personas se intoxican todos los años por culpa del mal uso de los datos personales. Abundan las historias de pornovenganza, humillación en línea, exposición de intimidades y otras violaciones del derecho a la privacidad. No solo los sujetos de datos sufren las consecuencias. Los desastres de ese tipo también pueden dañar a gobiernos y a empresas.

INSTITUCIONES INTOXICADAS

La vulnerabilidad relacionada con los datos se extiende también a las instituciones que los guardan y los analizan. Todo dato puede desencadenar un desastre que merme la rentabilidad de una compañía, perjudique su imagen, reduzca su cuota de mercado, dañe su valor en bolsa y desemboque en

potenciales demandas judiciales muy costosas o incluso en acusaciones penales. Las organizaciones que acaparan más datos de los necesarios están generando su propio riesgo.

Es cierto que no todas las compañías se arruinan con los desastres relacionados con los datos. Algunas han tenido suerte. A Ashley Madison, por ejemplo, le va mejor que nunca. Facebook ha sobrevivido a innumerables pifias de ese tipo, aunque no sin que hayan hecho mella en su imagen. Puede que todavía tengamos la sensación de que hay que estar en Facebook por una necesidad social o profesional, pero ya no «mola». Y eso, por sí solo, podría significar a largo plazo la sentencia de muerte para esa plataforma. Es una empresa que puede enfrentarse a serios problemas en cuanto una competidora ofrezca una alternativa seria. En nuestra reciente encuesta antes mencionada, las personas consultadas consideraban que Facebook era el menos fiable de todos los gigantes tecnológicos; daban a la compañía una puntuación media de 2,75 sobre una escala que iba del 0 («No me fío para nada de ellos») al 10 («Confío completamente en ellos»). [15]

Nadie se sorprendería si Facebook acabara perdiendo su posición de poder como consecuencia de su falta de consideración hacia la privacidad. Eso está aún por ver. Facebook sigue en pie, aunque pertenecer (o haber pertenecido) a su plantilla de empleados se haya convertido en un motivo de vergüenza más que de orgullo para algunos. Cuando empecé a estudiar el tema de lo digital, quienes trabajaban en ese gigante de las redes sociales solían alardear de sus empleos. Hoy no es extraño que la gente guarde silencio sobre sus vínculos con la compañía del pulgar azul. [16]

El que haya empresas que logren sobrevivir a un desastre relacionado con los datos no significa que todas lo hagan. Gestionar datos sensibles es como manejar cualquier otra sustancia tóxica. Cuando algo sale mal, puede suponer la muerte de la compañía. He ahí el caso de Cambridge Analytica. Dos meses después de que se revelara que había intentado influir en campañas electorales de todo el mundo utilizando datos personales, la firma solicitó un concurso de acreedores por insolvencia y tuvo que cerrar. También Google clausuró su red social Google+ a raíz de que se revelara que unos defectos de diseño de su *software* habían permitido que desarrolladores externos accedieran a los datos personales de los usuarios.

Aun en el caso de que estas organizaciones sigan adelante tras un escándalo, sobrevivir a una intoxicación por datos puede salir muy caro. Hasta la fecha, a Facebook se le han impuesto sanciones por un monto total de 5.000 millones de dólares por sus múltiples transgresiones de la privacidad, [17] a las que cabe sumar medio millón de libras en Reino Unido por el escándalo de Cambridge

Analytica. Y eso fue antes de que entrara en vigor el actual Reglamento General de Protección de Datos (RGPD) de la Unión Europea. [18] Según esta nueva regulación, las multas pueden ser de 20 millones de euros o un 4 por ciento de los ingresos (el que sea mayor de esos dos importes), y Facebook está siendo objeto en estos momentos de varias investigaciones paralelas con arreglo a dicha normativa. En 2019, la Oficina del Comisionado de Información de Reino Unido anunció su intención de multar a British Airways con 183 millones de libras en aplicación del RGPD por una filtración en sus sistemas de seguridad de datos que afectó a 500.000 clientes. [19] Mientras las organizaciones no cambien sus prácticas, seguiremos viendo multas cada vez más frecuentes y, posiblemente, más altas. Una buena regulación es aquella que procura armonizar los intereses de las empresas con los de los clientes. Si una negligencia con los datos perjudica a los usuarios, las compañías responsables tienen que sufrir un daño también.

A veces, un desastre en materia de privacidad no termina en multa, pero sí llega a dañar seriamente a una institución. Así ocurrió con un caso de violación de datos en la Oficina de Administración del Personal de Estados Unidos en 2015. Unos jáqueres robaron unos 21 millones de historiales de la administración estadounidense, entre los que se incluían investigaciones de antecedentes de miembros actuales, antiguos o potenciales del personal federal. Entre los datos sensibles que se perdieron, había nombres, domicilios, fechas de nacimiento, historiales de empleo y salariales, resultados de detectores de mentiras, informes de conductas sexuales de riesgo, y más de 5 millones de juegos de huellas digitales. Todos esos historiales robados se podrían utilizar, por ejemplo, para destapar a investigadores infiltrados. [20] Violaciones de datos como esta no solo dañan la reputación de quien las sufre, sino que también ponen en riesgo la seguridad de todo un país.

SOCIEDADES INTOXICADAS

Hay cuatro principales vías por las que la mala gestión de los datos personales puede intoxicar a las sociedades. Los datos personales pueden comprometer la seguridad nacional, pueden usarse para corromper la democracia, pueden ser una amenaza para las sociedades liberales si se utilizan para fomentar una cultura de exhibición de las intimidades y de vigilantismo, y pueden representar un peligro para la seguridad de los individuos.

Amenazas para la seguridad nacional

Equifax es uno de los mayores brókeres de datos y una de las grandes agencias elaboradoras de informes de crédito de consumidores que hay en el mundo. En septiembre de 2017, anunció que había detectado una brecha de ciberseguridad por el que unos delincuentes habían accedido a los datos personales de unos 147 millones de ciudadanos estadounidenses. Entre la información a la que tuvieron acceso había nombres, números de la seguridad social, fechas de nacimiento, direcciones y números de carnet de conducir. Es una de las mayores violaciones de datos de la historia. Hasta aquí, bastante preocupante. Pero en febrero de 2020, la historia dio una nueva (y más sombría) vuelta de tuerca cuando el Departamento de Justicia de Estados Unidos acusó formalmente a cuatro militares chinos de nueve cargos penales relacionados con aquella filtración (en la que China ha negado hasta el momento toda implicación).

¿Para qué querrían las fuerzas armadas chinas todos esos datos personales? Una posibilidad es que quisieran identificar a posibles objetivos para reclutarlos como espías. Cuanta más sea la información de que se dispone sobre las personas, más probable será conseguir lo que se quiera de ellas. Si se les descubre un secreto, se las puede chantajear. Si se estudia su psicología, se puede anticipar qué las motiva.

Se sabe que China utiliza redes sociales como LinkedIn para reclutar a espías. LinkedIn tiene 645 millones de usuarios que buscan en ella oportunidades de empleo y que, por lo tanto, están abiertos a ser contactados por desconocidos. Las personas que han trabajado alguna vez para organismos del Estado a veces anuncian su habilitación personal de seguridad para mejorar sus posibilidades de encontrar trabajo. Toda esa información y esa facilidad de acceso tienen un gran valor para los espías chinos. Es mucho menos arriesgado y mucho más eficiente en cuanto a costes contactar en línea con candidatos potenciales que hacerlo en persona. Se cree que los espías chinos han tratado de establecer comunicación con miles de ciudadanos alemanes y franceses a través de las redes sociales. [21]

Una segunda razón por la que los países extranjeros pueden desear datos personales de otras naciones es su interés por entrenar a sus algoritmos. China dispone de montañas de datos sobre sus ciudadanos, pero no sobre otras personas del resto del mundo, y los algoritmos entrenados con datos de individuos de su propio país podrían no funcionar bien con los occidentales. Una tercera razón es el deseo de usar esos datos para diseñar campañas de desinformación dirigidas, como hizo Cambridge Analytica. Y, por último, los datos son una mercancía que se puede vender a otros gobiernos. [22] Tal vez Rusia o Corea del Norte estén igual de interesadas que China por saber más sobre los estadounidenses.

El ataque a Equifax fue llevado a cabo por profesionales. Los jáqueres robaron

la información en tomas reducidas para no ser detectados y enrutaron los datos de su tráfico por internet a través de treinta y cuatro servidores distintos de más de una docena de países para cubrir sus huellas. Sin embargo, al parecer, Equifax no tuvo el debido cuidado. En la demanda colectiva presentada posteriormente por los afectados contra la empresa, se alegó que esta tenía información sensible almacenada en archivos de texto sin cifrar, de fácil acceso, y que, en al menos uno de los casos, la compañía había usado una contraseña muy débil («admin») para proteger uno de sus portales. Similar importancia tuvo el hecho de que no hubiera actualizado su software de Apache Struts. [23] Apache había hecho pública la detección de una vulnerabilidad en su software y había ofrecido a sus usuarios un parche, pero Equifax no lo había instalado. [24]

En el caso de Equifax, lo que se produjo fue un robo de datos. Pero debido a la proliferación de brókeres de datos, hoy estos pueden comprarse legalmente y usarse con fines igualmente perversos. Cuando los datos de ubicación que guardaba un bróker de datos llegaron a la redacción de *The New York Times* enviados por unas fuentes «alarmadas ante el uso abusivo que de ellos se podría hacer», unos periodistas del diario investigaron hasta qué punto podían ser peligrosos. [25] Los datos incluían información sobre unos 12 millones de teléfonos en Estados Unidos. Entre las zonas sensibles visitadas por algunas de las personas rastreadas había instalaciones de terapia psicológica, clínicas de metadona, espacios *queer* , iglesias, mezquitas y clínicas de interrupción del embarazo. Alguien que trabajaba en el Pentágono había visitado una institución especializada en salud mental y en el tratamiento de adicciones en más de una ocasión. Los periodistas llegaron a identificar y seguir a oficiales militares con habilitaciones personales de seguridad importantes, así como a agentes de cuerpos policiales. Valiéndose de los emplazamientos de las bases militares estadounidenses como guía, lograron deducir el cargo de un mando de la Fuerza Aérea de Estados Unidos. Más alarmante aún fue el que solo les llevara unos minutos desanonimizar los datos de ubicación y rastrear al mismísimo presidente Trump (a través del teléfono de un agente del servicio secreto). [26] Si cualquiera de esas personas tiene algo que ocultar (como lo tenemos todos), tal facilidad de acceso a sus datos las convierte en blancos fáciles de un chantaje. En el peor de los casos, los datos de ubicación podrían facilitar el secuestro o el asesinato de una persona. Si quienes están a cargo de la seguridad de nuestros países son gente fácil de encontrar, seguir y poner potencialmente en peligro, entonces todos estamos en riesgo, y los agentes extranjeros son muy conscientes de cómo los datos personales hacen vulnerables a los países.

La preocupación por la seguridad nacional fue lo que llevó a Estados Unidos a presionar a TikTok, una red social china, para que vendiera su filial occidental a

una empresa estadounidense en 2020. [27] Antes, Estados Unidos había obligado también al gigante de los juegos digitales Beijing Kunlun a vender su participación en Grindr a una compañía estadounidense. Grindr es una app de citas orientada al público homosexual, bisexual y transexual. Almacena datos extraordinariamente delicados que incluyen conversaciones eróticas, fotos y vídeos de desnudos, ubicaciones en tiempo real, direcciones de correo electrónico y resultados de las pruebas del VIH. Si viviéramos en un mundo en el que la privacidad fuera algo que se toma en serio, una aplicación así estaría obligada a ofrecer garantías de ciberseguridad y privacidad a prueba de fuego. No te sorprenderá saber que ese no es el caso. En 2018, una organización noruega dedicada a la investigación descubrió que Grindr enviaba datos personales —incluidos los referidos a si la persona es portadora o no del VIH— a terceros que ayudan a mejorar la app. Según el informe, buena parte de esos datos —los de ubicación, por ejemplo— se enviaban sin cifrar a distintas compañías publicitarias. [28]

Estados Unidos no reveló detalles sobre los aspectos de Grindr que habían suscitado su preocupación —tal revelación «podría haber llevado potencialmente a desvelar conclusiones confidenciales elaboradas por agencias federales estadounidenses», aseguró una fuente—, pero, a la vista del contexto del caso, no resulta difícil imaginar cuáles fueron. A fin de cuentas, Kunlun había facilitado a ingenieros ubicados en Pekín acceso a la información personal de millones de estadounidenses (incluidos sus mensajes privados). [29] Es probable que algunos miembros de las fuerzas armadas y las agencias de inteligencia de Estados Unidos usen la aplicación, por lo que China podría utilizar sus datos para chantajearlos, o para inferir movimientos de tropas estadounidenses. [30] No sería la primera vez que una app revela movimientos de efectivos.

La mayoría de las personas que salen a correr lo hacen cerca de su casa o de su trabajo, y quienes trabajan en proyectos ultrasecretos del Gobierno no son ninguna excepción. Cuando miembros del personal militar estadounidense compartieron sus recorridos con Strava, una empresa especializada en *fitness* , no cayeron en la cuenta de que estaban anunciando la ubicación de bases secretas del ejército. Strava publicó los recorridos de todos los corredores que usaban su aplicación en un mapa de calor en su sitio web. Era un mapa que se podía ampliar para estudiar más de cerca las zonas más y menos transitadas por los *runners* . Los analistas señalaron que, no solo se podía inferir dónde estaban situadas ciertas bases secretas del ejército (por estar enmarcadas por rutas en zonas que por lo demás mostraban una densidad de actividad baja), sino que también se podía identificar a usuarios de Strava por su nombre cruzando su información con la de otras bases de datos públicas. A partir del mapa de calor,

se podía identificar y hacer un seguimiento de personal militar de interés. [31]

En este caso, los datos que provocaron una amenaza para la seguridad nacional no fueron ni siquiera robados o comprados; eran públicos y fácilmente accesibles. Tras el incidente, Strava hizo más visible y simple su función para que el usuario pudiera excluirse voluntariamente de aparecer en los mapas de calor. [32] Fue un gesto demasiado pequeño que llegaba demasiado tarde. Los usuarios tendrían que optar de manera voluntaria para que se recolectaran sus datos. La falta de respeto generalizada por la privacidad hace que los datos personales de militares y funcionarios del gobierno también estén en riesgo. A través de esas personas, las potencias extranjeras pueden hacer que peligre la seguridad de todo un país.

Amenazas a la democracia

El escándalo de Cambridge Analytica ilustra cómo las pérdidas de privacidad pueden propiciar la manipulación de la democracia. Las violaciones de la privacidad posibilitaron la construcción de perfiles que se usaron para dirigir propaganda adaptada a cada persona, en sintonía con sus tendencias psicológicas. Christopher Wylie, que denunció desde dentro las prácticas de Cambridge Analytica, está convencido de que el Brexit no habría ganado en el referéndum si la empresa especializada en datos no hubiera interferido en el proceso. [33] De cierta forma, la compañía dañó a todos los ciudadanos de los países en los que interfirió, pero también a los de otras naciones, dado que a todos nos afecta la política mundial. Así de amplia es la repercusión que los daños relacionados con el mal uso de los datos pueden tener.

Chris Sumner, director de investigación y cofundador de la Online Privacy Foundation, una organización sin ánimo de lucro, lideró un estudio sobre los «anuncios oscuros», así llamados porque solo son visibles para quien los publica y para el destinatario al que van dirigidos de forma específica. Se pueden crear grupos de estos destinatarios con datos sobre ubicación, conducta e información psicográfica. (Los perfiles psicográficos clasifican a los individuos según unos tipos de personalidad basados en los datos personales.) Sumner quiso probar hasta qué punto puede ser efectiva esa personalización. Él y su colaborador, Matthew Shearing, evaluaron la propensión al autoritarismo de 2.412 personas en Facebook, a las que dividieron en dos grupos: las de tendencia autoritaria alta y las de tendencia baja. Las personalidades autoritarias se caracterizan por una inclinación a obedecer y a respetar a las personas que ostentan posiciones de autoridad, valoran más las tradiciones y las normas y son también menos

tolerantes con aquellos que no pertenecen a su propio grupo. Sumner y Shearing crearon anuncios a favor o en contra de la vigilancia estatal masiva.

El equipo investigador diseñó cuatro campañas publicitarias diferentes. El anuncio provigilancia dirigido a personas con una alta tendencia autoritaria mostraba la imagen de unos edificios bombardeados, acompañada del mensaje siguiente: «Terroristas. No dejes que se escondan en línea. Di sí a la vigilancia masiva». La versión creada para personas con bajas tendencias autoritarias era: «La delincuencia no se detiene ante internet. Di sí a la vigilancia». Por su parte, el anuncio antivigilancia personalizado para individuos con altos niveles de autoritarismo enseñaba la imagen de los desembarcos del día D y el mensaje: «Lucharon por tu libertad. ¡No la eches por tierra! Di no a la vigilancia masiva». Y en la versión diseñada a medida de las personas con niveles reducidos de autoritarismo aparecía una fotografía de Ana Frank con el mensaje: «¿De verdad piensas que no tienes nada que temer si no tienes nada que esconder? Di no a la vigilancia estatal».

Los anuncios diseñados a medida se mostraron más eficaces en los grupos de destinatarios a los que iban dirigidos. El anuncio a favor de la vigilancia y focalizado en personalidades con un alto componente autoritario, por ejemplo, fue compartido o aprobado con un «me gusta» veinte veces más por miembros del grupo de autoritarismo elevado que por miembros del de autoritarismo bajo. La probabilidad de que las personas clasificadas como muy inclinadas al autoritarismo compartieran un anuncio diseñado para ellas era significativamente mayor, mientras que las personas clasificadas como de bajas tendencias autoritarias encontraron los anuncios diseñados para ellas mucho más persuasivos que los ideados para sus contrarias. [34] Lo que no está claro, sin embargo, es cómo esos indicadores (la probabilidad de compartir una publicación o de considerar persuasivo un anuncio) se traducen en votos.

Algunos escépticos defienden que la microfocalización tiene efectos limitados y que, por lo tanto, su impacto en las elecciones no debería preocuparnos. Una dificultad importante a la que se enfrentan las campañas que intentan influir en las opiniones de las personas es que no siempre hay una correlación fuerte entre los rasgos de personalidad y los valores políticos de los individuos. Si las campañas se equivocan al valorar a las personas, pueden errar el blanco de los mensajes y sufrir una reacción adversa. Otro problema que se les presenta es que el poder predictivo de los «me gusta» de Facebook tiene fecha de caducidad; lo que te gustaba hace cinco años puede no ser lo que te guste ahora, pero nunca te molestaste en desmarcar tus «me gusta» del pasado. Además, el que ahora «te guste» algo puede tener un significado diferente del que tendrá dentro de un año. Que «te guste» un político antes y después de un suceso político de importancia,

como fue, por ejemplo, el referéndum del Brexit, puede indicar posturas políticas muy diferentes. Las campañas políticas también se enfrentan, además, a la competencia de otras campañas que emplean tácticas idénticas, por lo que, como mínimo, algunos de los efectos pueden anularse mutuamente. [35]

Lo preocupante, sin embargo, es que la microfocalización sí tiene un impacto, por limitado que sea. Los estudios al respecto indican, por ejemplo, que cuando se dirige a un votante contenido de un partido contrario que hace hincapié en un tema concreto en el que el votante y el candidato político están de acuerdo, es más probable que esa persona vote a ese partido o se abstenga de votar. [36]

Cuando las personas expuestas a propaganda personalizada se cuentan por millones, no hace falta que el efecto sea muy grande para inclinar la balanza de unas elecciones. En 2012, Facebook publicó en *Nature* los resultados de un estudio controlado aleatorizado con 61 millones de usuarios residentes en Estados Unidos realizado durante las elecciones al Congreso de 2010. (Fiel al estilo de Facebook, parece que el estudio se llevó a cabo sin el consentimiento informado de sus participantes.) [37] El día de los comicios, se mostró a un grupo un mensaje en el encabezamiento de sus noticias en el que se animaba a sus miembros a votar y que iba acompañado del botón clicable «Yo ya he votado». A los de otro grupo se les mostró el mismo mensaje, pero con hasta seis fotografías de perfil de sus amigos en Facebook que ya habían hecho clic en el icono de «Yo ya he votado». Los usuarios de un tercer grupo, el de control, no recibieron mensaje alguno. Los resultados muestran que entre quienes recibieron el mensaje acompañado de las fotografías de amigos se registró un 0,4 por ciento más de probabilidades de votar. Puede que no parezca una gran diferencia, pero cuando son millones las personas expuestas a un mensaje o una imagen que les influye, los números se acumulan. Los autores del estudio dijeron haber aumentado la participación electoral total en unos 340.000 votos. [38]

Si te pones a pensar en cuántas elecciones se ganan por un margen alarmantemente bajo de sufragios, 340.000 votos parecen más que suficientes para dar un vuelco a unos comicios. En Estados Unidos, Trump ganó las elecciones de 2016 por una estrecha diferencia de 70.000 votos en tres estados de pronóstico incierto. [39] En el referéndum del Brexit, la salida de la Unión Europea ganó por un margen de menos del 4 por ciento de los votos. Que Facebook animase a todos sus usuarios a votar podría no ser algo malo. Pero ¿y si animara únicamente a unas personas, y no a otras? ¿Y si esas personas no fueran elegidas al azar, sino fueran aquellas más propensas a votar a un partido determinado? Uno de los objetivos de Cambridge Analytica era identificar a electores «fáciles de persuadir»: aquellos a los que se podía convencer para que no fueran a votar o para que votaran a un candidato al que, de otro modo, no

votarían. A algunas de esas personas se les mostraban noticias falsas sobre el candidato al que trataban de perjudicar, a otras se les enseñaban contenidos que las desanimaran para que no acudieran a las urnas, etcétera.

Un reciente documental de Channel 4 mostró que la campaña electoral de Trump para las presidenciales de 2016 categorizó a más de 3,5 millones de estadounidenses negros como potencialmente susceptibles de disuasión. El documental describe la clase de datos que la campaña tenía sobre casi 200 millones de electores; cosas como «si tiene un perro o una pistola, si es probable que se case, si tiene previsto tener hijos; había incluso puntuaciones por tipo de personalidad». El documental da a entender que, a juzgar por el desplome de la participación en estados clave, la campaña puede haber sido exitosa, aunque otros factores también entraron en juego. Ver la reacción de aquellos ciudadanos negros cuando se les enseña cómo se los había etiquetado como objetivos de disuasión, y cuáles eran los datos que el equipo de campaña tenía sobre ellos, es inquietante. Muchos de los anuncios diseñados para desincentivar el voto eran anuncios oscuros en Facebook. Según el documental, la campaña de Trump gastó 44 millones de dólares en la emisión de 6 millones de anuncios diferentes en la plataforma de la red social. Facebook mantiene secreto el contenido de esos anuncios. [40]

Que una empresa como Facebook tenga ese poder para influir en el electorado es algo que debería preocuparnos. Como los propios autores del estudio sobre Facebook señalan, la carrera de las presidenciales estadounidenses de 2000 entre Al Gore y George W. Bush se decidió por solo 537 votos en Florida, menos del 0,01 por ciento de los votos emitidos en ese estado. Si Facebook hubiera animado a los electores demócratas de Florida a acudir a las urnas y no hubiera hecho lo mismo con los republicanos, lo más probable es que Al Gore hubiera salido elegido presidente, y la historia habría seguido un curso completamente distinto.

Los botones de voto en Facebook se han usado en el referéndum sobre la independencia de Escocia de 2014, el referéndum irlandés de 2015, las elecciones generales británicas de ese año, el referéndum del Brexit de 2016, las elecciones estadounidenses de 2016, y las elecciones federales alemanas y las parlamentarias islandesas de 2017. Al menos en Islandia, no se les mostraron esos botones a todos los ciudadanos usuarios de la red social, pero desconocemos cuántas personas vieron el botón o qué criterios se siguieron para decidir quién podía verlo y quién no. *Simplemente no sabemos qué efecto han tenido esos mensajes en nuestras elecciones* . Facebook se reserva esa información para sí. [41] El que una de las corporaciones más poderosas del planeta sepa tanto de nosotros y que permitamos que nos muestre mensajes que

pueden influir en nuestro comportamiento electoral es una locura —sobre todo si ni siquiera la auditamos. Deberíamos tomarnos más en serio el que se pueda manipular la democracia de ese modo.

Uno de los pilares más importantes de una democracia sana es la celebración de elecciones limpias. No solo eso; la gente debe estar convencida de que lo son. Si la mayoría de los ciudadanos sospecharan que se producen interferencias en el proceso electoral, la legitimidad del gobierno podría quedar seriamente en entredicho.

Había algunos motivos para preocuparse por la posibilidad de nuevas interferencias electorales relacionadas con Facebook durante la carrera presidencial estadounidense de 2020. En primer lugar, casi un 70 por ciento de la población adulta de Estados Unidos usa Facebook. [42] La red social tiene, pues, potencial para influir en la mayoría del electorado estadounidense. [43]

En segundo lugar, Facebook ha demostrado ser muy poco de fiar, como se ha señalado a lo largo de este libro, fallando a sus usuarios tantas veces que cuesta llevar la cuenta. [44]

En tercer lugar, aunque Facebook ha introducido algunos cambios positivos dirigidos a una moderación de la publicidad de contenido político, sus políticas en ese terreno siguen siendo muy cambiantes, autoimpuestas, autosupervisadas y controvertidas. [45] Facebook no solo ha permitido mentiras y bulos, sino que también los ha priorizado, dado que esos anuncios pagados tienen acceso a herramientas —como la microfocalización— que maximizan su influencia. [46] Las democracias modernas no han desarrollado todavía unas políticas consolidadas, con aval estatal y supervisión independiente, que regulen las campañas políticas en las redes sociales. Facebook no puede autocorregirse, porque su modelo de negocio no se lo permite. Siempre le convendrá tener contenidos incendiarios que atraigan la atención de los usuarios durante más tiempo. [47] La economía de datos propicia las *fake news* . Cuando aún no había transcurrido un mes desde las elecciones, se publicó un estudio realizado en el marco del proyecto Digital New Deal del *think tank* German Marshall Fund, en el que se indicaba que «el nivel de atención dedicada a artículos de medios que publican de forma reiterada contenidos que se han comprobado falsos» en Facebook se había incrementado un 102 por ciento durante los meses previos a las elecciones de 2016. [48]

Y en cuarto (y más importante) lugar, Facebook tenía un especial interés en el resultado de esas elecciones porque quería evitar la regulación de su sector, y eso hacía que se sintiera más tentado aún a interferir.

La contratación para varios de sus puestos de alta dirección de antiguos cargos republicanos y su propio deseo de mantener desregulado su terreno de juego dio

pie a ciertas muestras de preocupación por el posible sesgo conservador de Facebook. [49] La realidad es que, si hubiese querido, Facebook podría haber interferido en las elecciones sin haber tenido que rendir cuenta alguna por ello. O podría haber permitido que otros actores —como ciertos partidos rusos, por ejemplo— lo hicieran. Puede que ni siquiera hubiéramos llegado a saber si algo así hubiera ocurrido, a menos que alguien lo hubiera denunciado desde dentro o se hubiera llevado a cabo una investigación seria del asunto. [50]

Es muy probable que Facebook haya actuado de forma responsable y se haya abstenido de interferir en las elecciones de 2020, incluso a costa de su interés por impulsar la desregulación. Pero no tendríamos que fiarnos de que Facebook ni ninguna otra compañía vayan a respetar nuestros procesos democráticos. El Estado de derecho no puede depender solo de la buena fe. La democracia solamente puede ser robusta si nadie puede interferir impunemente en unas elecciones.

Fue inquietante ver a plataformas como Twitter y Facebook inventándose nuevas políticas para tratar de frenar la preocupante evolución de los acontecimientos en torno a las elecciones de 2020. Era como si una democracia que juzgábamos sólida y experimentada tuviera que ir reaprendiendo sobre la marcha a garantizar la seguridad y la limpieza de las elecciones. Muchas de las políticas puestas en práctica por las plataformas de redes sociales parecían parches improvisados, respuestas poco estudiadas a las situaciones que se iban presentando. Más preocupante aún era la extraña sensación de ver a unas empresas privadas aplicando unas normas para intentar proteger el sistema democrático; empresas propietarias de plataformas que, hasta ese momento, habían contribuido a erosionar la democracia. Twitter y Facebook no parecen ser la clase de organización que cuenta con los conocimientos ni la legitimidad apropiados para elaborar las reglas en las que se deben enmarcar unos comicios democráticos. Una democracia fuerte requiere de unas herramientas más estables, fiables, legítimas y transparentes con las que garantizar unas elecciones seguras y limpias. Y esas normativas no pueden ser impuestas por empresas privadas; da igual lo bien intencionadas que puedan ser. No cabe duda de que, a falta de unas reglas democráticas legítimas del conjunto de la sociedad que regulen las campañas políticas en línea, que las plataformas de redes sociales intenten limitar la desinformación y las posibles injerencias en las elecciones es mejor que nada, pero no es suficiente. No podemos dejar nuestras democracias en manos de corporaciones privadas que son igual de capaces de ayudar a la democracia como de socavarla, si les interesa económicamente.

No podemos permitir que lo que ocurrió con Cambridge Analytica suceda de nuevo. Aunque no está claro hasta qué punto las actividades de esa empresa y

otras por el estilo lograron su objetivo de influir en las elecciones, lo que sí es palmario es que la intención de Cambridge Analytica era boicotear la democracia. [51] Quería jaquear al electorado. No trataba de difundir información veraz y dar buenos argumentos sobre por qué debíamos votar a un candidato o a otro, sino que apelaba a las emociones más primarias de las personas, sin escrúpulo alguno por la verdad, mostrando contenidos muy distintos a individuos muy diferentes entre sí. Desanimar a las personas para que no vayan a votar porque podrían apoyar al candidato al que tú estás intentando derrotar equivale a boicotear la democracia. Es jugar sucio. Es muy posible —quizá incluso probable— que tanto el Brexit como Trump hubieran perdido de no haber sido por los anuncios políticos personalizados que se introdujeron en las redes sociales. Sin embargo, aun si ese no fue el caso, el simple intento de jaquear la democracia es algo que debemos detener, igual que hemos de poner freno a los intentos de asesinato, aunque siempre exista la posibilidad de que no logren su objetivo.

Tal vez te preguntes qué diferencia hay —si es que existe alguna— entre la publicidad política microfocalizada que se basa en los datos personales y los anuncios de las campañas electorales de toda la vida. A fin de cuentas, ni la propaganda ni los mensajes políticos falsos se inventaron en la era digital. Lo novedoso (y destructivo) de la microfocalización es que muestra a cada persona una información diferente y potencialmente contradictoria. Las compañías de datos tratan de explotar nuestros rasgos propios de personalidad para decirnos aquello que queremos (o necesitamos) oír para que nos comportemos como quieren que lo hagamos. Un candidato podría dar una imagen ante unos ciudadanos y otra totalmente opuesta ante otro grupo distinto de estos sin que los unos ni los otros se den cuenta de ello.

Los anuncios personalizados fracturan la esfera pública en varias realidades paralelas. Si cada uno de nosotros vive en una realidad diferente porque se nos expone a contenidos enormemente distintos, ¿qué posibilidades tenemos de mantener debates políticos sanos? Cuando los políticos tienen que diseñar un mismo anuncio para el conjunto de la población, tienden a ser más razonables y a apelar a argumentos que probablemente sean aceptables para la mayoría de la ciudadanía. Es más probable que los anuncios personalizados sean extremos.

Cuando todos vemos los mismos anuncios, podemos comentarlos juntos. Periodistas, académicos y adversarios políticos pueden verificarlos y criticarlos. Los investigadores pueden tratar de medir su impacto. En la actualidad, los datos sobre anuncios y campañas electorales son privados, lo que hace difícil o imposible que los investigadores puedan acceder a ellos. [52] El escrutinio presiona a los candidatos políticos para que sean coherentes. Además, cuando

los anuncios son públicos, podemos controlar más fácilmente que los partidos políticos no gasten más de lo permitido y que no se anuncien en formas que están fuera de los límites de la ley. La publicidad electoral está muy regulada en otros medios como la televisión y la radio. En Reino Unido, está casi prohibida, salvo por un número muy restringido de aburridos «espacios reservados a los partidos políticos». Solo podemos regular esa publicidad si podemos verla, y por eso los anuncios oscuros y personalizados tienen que desaparecer. (Habrá más información sobre anuncios en el capítulo siguiente.)

Cuando las plataformas de redes sociales nos piden que compartamos nuestros datos para clasificarnos como viejos o jóvenes, hombres o mujeres, conservadores o progresistas, blancos o negros, proinmigración o antiinmigración, proabortistas o antiabortistas, con el fin de tratarnos en función de esas categorías, crean y consolidan divisiones. No debemos permitir que la esfera pública se desgarre y se escinda por las costuras que unen aquello que nos hace diferentes. No tiene por qué ser así. Para que todos nos sintamos cómodos en la esfera pública, para que, a pesar de nuestras diferencias, convivamos en armonía, para que el pluralismo sea posible, nuestra vida colectiva debe conservar un cierto grado de neutralidad, y para eso necesitamos el liberalismo.

Amenazas al liberalismo

El principio básico de las sociedades liberales es que los individuos deben tener la libertad de vivir sus vidas como crean oportuno. Existe una presunción a favor de la libertad, de modo que «la carga de la prueba corresponde a quienes [...] propugnan cualquier restricción o prohibición», como John Stuart Mill escribió. [53] Deben instaurarse normas que eviten daños para las personas, que garanticen que los ciudadanos vivan libres de injerencias innecesarias y que establezcan una vida en común en la que todos podamos participar. La privacidad es importante para construir una esfera privada fuerte, una burbuja de protección frente a la sociedad en la que los individuos puedan disfrutar de un tiempo y un espacio libres de las miradas, juicios, preguntas e intromisiones de otros. Las normas de privacidad cumplen la valiosa función de darnos un respiro. Se necesita un cierto grado saludable de reserva y ocultación para que la vida civilizada funcione sin grandes complicaciones. [54] Si todos pudiéramos saber lo que piensan los demás en todo momento, la esfera privada se reduciría a nada y el ámbito público se contaminaría con interminables e innecesarios conflictos. El liberalismo no se reduce a la no injerencia de los estados en las vidas privadas de los ciudadanos. Para que el liberalismo prospere, debe estar integrado en una

cultura análoga de contención en la que los ciudadanos de a pie se esfuercen por dejarse tranquilos los unos a los otros.

Las redes sociales nos animan a «compartir» en línea. El modelo de negocio de Facebook depende de que las personas revelen aspectos de sí mismas en su entorno digital. Cuando los usuarios no comparten tantos contenidos personales, Facebook se preocupa y ajusta la plataforma para incitarnos a compartir más. [55] Comparte todo lo que puedas, es el mensaje. Dinos quién eres, dinos cómo te sientes, háblanos de tu familia y amigos, cuéntale al mundo qué opinas de otras personas. Queremos saberlo. Queremos oír todo lo que tengas que decir.

Las plataformas de las redes sociales fomentan una cultura que disuade a las personas de callarse. Cuanto más compartan, más datos podrán analizarse y usarse para vender acceso a nosotros. Cuantos más comentarios hagan las personas sobre lo que otras comparten, más clics, más anuncios, más dinero y más poder. Puede parecer una situación en la que todos salimos ganando. Nosotros podemos despotricar lo que queramos y las compañías tecnológicas hacen negocio. Pero buena parte de lo que se comparte en línea no beneficia a los usuarios. A tus datos se les saca un provecho que a ti, como usuario, no te interesa, y lo que compartes te expone ante otros usuarios, algunos de los cuales están encantados de trolearte, chantajearte o humillarte. Las redes sociales son comunicación sin restricciones. Sin embargo, la civilidad exige un punto de contención en lo que compartes sobre ti mismo, en las opiniones que expresas (especialmente sobre otras personas) y en las preguntas que haces. La autocontención no tiene por qué equivaler a la deshonestidad. Del mismo modo que la ropa no engaña a los demás acerca de que estás desnudo por debajo, no expresar lo estúpida que crees que es otra persona tampoco equivale a mentir. No es necesario saberlo todo sobre otra persona para mantener una conversación franca. No necesitamos conocer los temores más oscuros, los secretos y las fantasías de las otras personas para trabar amistad con ellas, y menos aún para ser buenos vecinos. No queremos contárselo todo a nuestros conciudadanos. E, igualmente importante, tampoco queremos saberlo todo de ellos.

Esperar que las personas sean santas en cuerpo, palabra y pensamiento en todo momento no es realista ni razonable. Como bien ha señalado el filósofo Thomas Nagel, «todo el mundo tiene derecho a cometer un asesinato en su imaginación de vez en cuando». [56] Si forzamos a las personas a compartir más de lo que lo harían en otras circunstancias, terminaremos con un entorno social más pernicioso que si las animamos a cuidar mejor de lo que aportan a la esfera pública. Una cultura de la exhibición nos empuja a compartir nuestros asesinatos imaginarios con el mundo y, al hacerlo, nos enfrenta entre nosotros sin necesidad. Ahorrarnos los unos a los otros nuestras facetas menos agradables no

es un defecto: es un acto de generosidad.

El liberalismo nos pide que nada esté sometido al escrutinio público más que lo estrictamente necesario para proteger a los individuos y cultivar una vida colectiva saludable. Una cultura de la exhibición obliga a que *todo* se comparta y se someta a la inspección pública. Las grandes tecnológicas venden la fantasía de que quienes no hacen nada malo no tienen nada que ocultar, que la transparencia siempre es una virtud. No lo es. El de los exhibicionistas que se muestran ante otras personas no es un comportamiento virtuoso. En la economía digital, todo el mundo se ve empujado a expresar más de lo que la amistad, la comunicación efectiva o el debate público requieren, todo en un esfuerzo por crear más datos.

Ese compartir en exceso beneficia a las grandes compañías tecnológicas, no a los usuarios. Convierte la esfera pública en un espacio inhabitable. Tan incesante presión social para que compartamos deriva en expresiones de agresividad e intolerancia, cuando no en vigilantismo y cazas de brujas. No hay tregua. Cada imagen, cada palabra, cada clic son recogidos y monetizados por las empresas, y examinados y potencialmente despedazados en un acto público catártico de humillación digital entre los internautas. Ese continuo alboroto en torno a cualquier detalle de lo que las personas dicen y hacen nos distrae de otras conversaciones más importantes sobre temas como la justicia, la economía, la ecología y los bienes públicos. Mientras andamos ocupados en interminables riñas en línea, troleándonos y haciendo trizas a cualquiera por mostrar debilidades humanas que probablemente compartimos, nuestras democracias se desmoronan.

En cierto sentido, estas culturas de la exhibición recuerdan a la brutalidad de las relaciones sociales durante la infancia. Es bien conocido que los niños no saben cuándo dejar de hablar, como famosa es también su potencial crueldad, sobre todo cuando están en grupo. Quizá a medida que internet vaya madurando, logremos distanciarnos de una cultura donde compartimos y acosamos en exceso, y nos acerquemos a formas más adultas de relacionarnos.

Amenazas a la seguridad de los individuos

A los datos personales se les puede dar, se les da y se les seguirá dando un mal uso. Y algunos de los usos abusivos de los datos personales son más mortíferos que el amianto.

Uno de los ejemplos más letales de abuso de los datos fue el del régimen nazi durante la Segunda Guerra Mundial. Cuando los nazis invadían un país,

enseguida se apoderaban de los registros locales como primer paso para controlar a la población y, en particular, para localizar a los judíos. Había mucha variación entre países, tanto en lo referente al tipo de registros que llevaba cada uno como a la reacción que mostraban ante aquella sed nazi de datos. La comparación más extrema es la que ofrecen los Países Bajos y Francia. [57]

Jacobus Lambertus Lentz no era nazi, pero hizo más por el régimen nacionalsocialista alemán que la mayoría de los más fervientes antisemitas. Era el inspector de registros de población holandés y su debilidad eran las estadísticas demográficas. Su lema era «Registrar es servir». En marzo de 1940, dos meses antes de la invasión nazi, propuso al Gobierno de su país la instauración de un sistema de identificación personal que obligara a todos los ciudadanos a llevar un carnet de identidad. La tarjeta utilizaba tintas traslúcidas que desaparecían a la luz de una lámpara de cuarzo, así como un papel con marca de agua, todo con el propósito de dificultar su falsificación. El Gobierno rechazó su propuesta con el argumento de que un sistema así sería contrario a las tradiciones democráticas holandesas, pues equivaldría a tratar a las personas comunes como si fueran delincuentes. Lentz se llevó una gran desilusión. Unos meses más tarde, volvió a proponer la misma medida, aunque, esta vez, a la Kriminalpolizei del Reich. Las fuerzas de ocupación estuvieron encantadas de ponerla en práctica. Todos los holandeses adultos pasaron a tener la obligación de llevar un carnet de identidad. En las tarjetas que llevaban los judíos se estampaba una «J»: una sentencia de muerte en sus bolsillos.

Además de los carnets, Lentz empleó máquinas Hollerith —aparatos tabuladores vendidos por IBM que se valían de tarjetas perforadas para grabar y procesar datos— para ampliar la información registrada sobre la población. En 1941, se emitió un decreto que obligaba a todos los judíos a inscribirse en su oficina local del censo. Durante décadas, los holandeses habían recopilado ingenuamente datos sobre la religión y otros detalles personales de sus ciudadanos con la idea de crear un sistema que pudiera hacer un seguimiento de cada individuo «desde la cuna hasta la tumba». Lentz y su equipo de colaboradores usaron las máquinas Hollerith y toda la información de la que disponían para facilitar a los nazis el seguimiento de personas.

En Francia, a diferencia de lo que ocurría en Países Bajos, los censos no recababan información sobre religión por razones de privacidad. El último censo que había recopilado datos de esa clase databa de 1872. Henri Bunle, jefe de la Oficina de Estadística General francesa, dejó claro a la Comisión General sobre Asuntos Judíos en 1941 que Francia desconocía cuántos judíos tenía y, más aún, dónde vivían. Además, Francia carecía de la amplia infraestructura de tarjetas perforadas de la que disponían los Países Bajos, lo que dificultaba la

recopilación de nuevos datos. Si los nazis querían que la policía llevara un registro de la población, esta tendría que hacerlo manualmente, con formularios de papel y fichas de cartulina.

Sin las tabuladoras Hollerith no había forma de clasificar y computar la información que se recopilaba sobre los ciudadanos. Los nazis estaban desesperados. René Carmille, que, además de auditor general del ejército francés, era un entusiasta de las tarjetas perforadas y poseía varias máquinas tabuladoras (incluidas algunas Hollerith), se ofreció como voluntario para poner orden en aquel caos y entregar a los judíos de Francia a sus verdugos.

Carmille desarrolló un número nacional de identificación personal que funcionaba como un código de barras descriptivo de cada individuo; fue el precursor del actual número de seguridad social francés. Se asignaron diferentes números para representar características personales como la profesión. Carmille también preparó el censo de 1941 para todos los ciudadanos franceses de entre catorce y sesenta y cinco años. En la pregunta 11 se pedía a los judíos que se identificaran a través de sus abuelos paternos y maternos y de la religión que profesaban.

Pasaron los meses y las listas de judíos que los nazis esperaban que Carmille les facilitara no llegaban. Los nazis se impacientaban. Comenzaron a practicar redadas contra judíos en París, pero, sin las tabulaciones de Carmille, dependían de que los judíos se entregaran ellos mismos, o fueran delatados por vecinos. Transcurrieron más meses y las listas siguieron sin llegar.

Los nazis no lo sabían, pero René Carmille nunca había tenido intención alguna de traicionar a sus conciudadanos. Era uno de los más altos cargos de la Resistencia francesa. Su operación generó unas 20.000 identidades falsas. Usó sus tabuladoras para identificar a personas que estaban dispuestas a combatir contra los nazis. Las respuestas a la pregunta número 11 sobre si los encuestados eran judíos jamás se tabularon. Los agujeros correspondientes nunca llegaron a perforarse y esos datos se perdieron para siempre. Hasta la fecha, se han descubierto más de 100.000 de aquellas tarjetas perforadas adulteradas; tarjetas que no llegaron a entregarse a los nazis. Cientos de miles de personas fueron salvadas por *una* sola persona que decidió *no* recopilar sus datos, sus datos tóxicos.

Parece razonable suponer que Carmille sabía que terminarían por descubrirle si no entregaba los datos que había prometido. Las SS lo arrestaron en 1944. Lo torturaron durante dos días y luego lo enviaron a Dachau, donde murió de extenuación en 1945.

La recopilación de datos puede matar. Los holandeses sufrieron la mayor tasa de mortalidad de habitantes judíos en la Europa ocupada: un 73 por ciento. De

una población estimada de 140.000 judíos holandeses, más de 107.000 fueron deportados, y 102.000 de ellos fueron asesinados. La tasa de mortalidad de los judíos en Francia fue del 25 por ciento. De una población estimada de entre 300.000 y 350.000, 85.000 fueron deportados y a 82.000 de estos los mataron. La falta de privacidad fue un factor decisivo para que murieran cientos de miles de personas en los Países Bajos, mientras que la protección de la privacidad salvó la vida de cientos de miles en Francia. Una prueba más que corrobora la hipótesis de que la recopilación de datos fue el factor que marcó la diferencia entre esos dos países nos la ofrece el hecho de que los judíos que se refugiaron en los Países Bajos sufrieron una tasa de mortalidad inferior a la de los judíos holandeses; los refugiados no estaban registrados. [58]

Otros casos documentados de usos indebidos de los datos personales son la expulsión en el siglo XIX de los indios americanos de sus tierras en Estados Unidos, la migración forzada de poblaciones minoritarias en la Unión Soviética en las décadas de 1920 y 1930, y el uso de un sistema de registro poblacional (instituido por los belgas en los años treinta del siglo XX) para localizar y asesinar a los tutsis durante el genocidio de Ruanda de 1994. [59]

El mejor indicador de que algo ocurrirá en el futuro es que haya ocurrido en el pasado. Estas historias no son de una galaxia lejana de un universo de ficción. Son historias reales de las que debemos aprender para no repetir los mortíferos errores del pasado. [60]

Imagina un régimen autoritario contemporáneo apropiándose de todos tus datos personales. Los déspotas del pasado disponían de retazos de información en comparación con los miles de datos a los que se puede acceder hoy sobre cualquier persona en el mundo con solo unos clics. Un gobierno autoritario podría conocer todos nuestros puntos débiles sin necesidad de poner mucho empeño en ello. Si pudiera predecir todos nuestros movimientos, podría ser el comienzo de un régimen invencible. Para que te hagas una idea de lo peligrosos que son los datos personales, imagínate un régimen como el nazi, pero en la actualidad, con acceso a datos en tiempo real sobre tu ubicación, tu perfil facial, tu forma de andar, tu frecuencia cardiaca, tus ideas políticas, tu afiliación religiosa y muchas cosas más.

Entre las muchas historias relacionadas con los datos que tuvieron lugar durante la Segunda Guerra Mundial, hay un caso que resulta particularmente instructivo. En marzo de 1943, una célula de la Resistencia holandesa lanzó un ataque contra el registro municipal de Ámsterdam. Su objetivo era destruir el mayor número posible de historiales y fichas para tratar de evitar el asesinato de 70.000 judíos de la ciudad. Gerrit van der Veen, Willem Arondéus, Johan

Brouwer, Rudi Bloemgarten y otros entraron en el edificio vestidos de policías. Sedaron a los guardias (perdonándoles así la vida), empaparon los archivos de benceno y prendieron fuego a los documentos. Varios simpatizantes de la causa pertenecientes al cuerpo de bomberos tenían conocimiento de que se produciría el ataque. Cuando sonó la alarma, hicieron todo lo posible por retrasar el despliegue de los camiones a fin de dar tiempo a que las llamas completaran la destrucción. Cuando llegaron al registro, utilizaron la máxima agua posible para dañar el mayor número de papeles.

Por desgracia, aquel ataque contra el registro no tuvo el éxito deseado. Doce miembros de aquella célula de resistentes fueron localizados y ejecutados. Y el incendio solo alcanzó a destruir un 15 por ciento de los documentos. [61]

Igual que los nazis sabían que tenían que ir a los registros para hallar información, los malhechores actuales también saben dónde encontrar nuestros datos. Y ni siquiera necesitan desplegar tropas e invadir un país para hacerse con nuestra información más sensible. Les basta con un buen jáquer. En ese sentido, el riesgo para nuestros datos personales y para todo aquello protegido por nuestra privacidad es mucho más elevado ahora que en el mundo anterior a internet.

Deberíamos aprender de los errores del pasado. Los datos personales son tóxicos y debemos regularlos como tales. No repitamos el error que cometimos con el amianto. Pusimos amianto en todas partes: en recubrimientos de frenos de automóviles, en tuberías, en baldosas y tejas, en el hormigón, en el cemento, en ladrillos, en la ropa, en colchones, en mantas eléctricas, en calentadores, en tostadoras, en tablas de planchar, en filtros de cigarrillo y en la nieve artificial, entre otros sitios. En cuanto estuvo incrustado en nuestros techos y paredes, en la propia estructura de los espacios que habitamos, se volvió muy difícil extraerlo sin correr riesgos. El amianto mata a cientos de miles de personas cada año. Sigue envenenando a seres humanos de todo el mundo, incluso en sitios donde ya está prohibido. [62]

No dejemos que los datos personales envenenen a los individuos, las instituciones y las sociedades. Por suerte para nosotros, todavía no es demasiado tarde para poder corregir nuestra trayectoria actual en lo referente a la información personal. Podemos enmendar internet y la economía. Aprendamos de la experiencia de los Países Bajos durante la Segunda Guerra Mundial. Los holandeses cometieron al menos dos grandes errores con respecto a la privacidad. Acumularon demasiados datos personales. Y, cuando se dieron cuenta de lo tóxicos que eran estos datos, no tuvieron una forma fácil y rápida de borrarlos. Nosotros estamos cometiendo esos dos mismos errores a una escala sin precedentes. Tenemos que cambiar eso antes de que sea demasiado tarde.

5

Desenchufar

La economía de la vigilancia ha ido demasiado lejos. Ha abusado de nuestra información personal en demasiados aspectos y ocasiones. Y la cantidad y la sensibilidad de los datos que se intercambian hacen que proseguir con este experimento a gran escala sea demasiado peligroso. Tenemos que poner fin al comercio de datos personales.

La economía de los datos tiene que desaparecer porque está reñida con las democracias libres, igualitarias, estables y liberales. Podemos esperar hasta que se produzca una catástrofe verdaderamente masiva (como una filtración monumental de datos biométricos —no olvidemos que, a diferencia de lo que ocurre con las contraseñas, nuestros rostros no son algo que podamos cambiar— o un mal uso de los datos personales con el objeto de perpetrar un genocidio) para que nos decidamos por fin a proteger la privacidad, o podemos reformar este tipo de economía ahora, antes de que sea demasiado tarde.

Los datos personales se han convertido en una parte tan importante de la economía que puede parecernos poco realista a estas alturas tratar de desenchufarla. Pero no olvidemos que también hubo un tiempo en que la idea de reconocer los derechos de los trabajadores sonaba igual de descabellada, o incluso más. En la actualidad, miramos al pasado y lamentamos la brutalidad de las prácticas de explotación laboral características, por ejemplo, de la Revolución Industrial. En el futuro, volveremos la vista atrás, hacia nuestros días, y lamentaremos la insensatez de la economía de la vigilancia.

Aunque los seres humanos no siempre destacamos por nuestra capacidad para prevenir los desastres, algunos ejemplos demuestran que somos capaces de coordinar nuestras acciones y rectificar una trayectoria equivocada. El ozono de las capas más externas de la atmósfera absorbe la mayor parte de los rayos ultravioleta procedentes del Sol. Sin una capa de ozono que nos proteja, nuestros ojos, nuestra piel, nuestro sistema inmune y nuestros genes se verían dañados por los rayos ultravioleta. A medida que la capa de ozono se fue adelgazando en la segunda mitad del siglo XX , aumentó la incidencia de cánceres de piel. En 1985, un grupo de científicos publicó un artículo en *Nature* en el que se describía el grado de destrucción anual de la capa de ozono sobre la Antártida. Íbamos directos al desastre.

Solo dos años después, en 1987, se firmó el Protocolo de Montreal, un acuerdo internacional que prohíbe la producción y el uso de sustancias químicas que dañan la capa de ozono, incluidos los CFC (clorofluorocarbonos). Estos compuestos químicos se usaban en todo el mundo en frigoríficos, aparatos de aire acondicionado y latas de aerosol. Eran atractivos por su reducido grado de toxicidad, de inflamabilidad (como en el caso del amianto) y de reactividad. Por desgracia, el que no reaccionen con otros compuestos también los convierte en peligrosos, porque eso alarga mucho su vida y, durante ese tiempo, pueden llegar a esparcirse por las capas altas de la atmósfera.

Gracias a la oposición de los expertos y de la población en general a la fabricación y utilización de los CFC, la industria innovó y encontró alternativas. Los agujeros y el adelgazamiento de la capa de ozono se han ido recuperando a un ritmo de entre un 1 y un 3 por ciento por década desde 2000. A este paso, la capa de ozono que cubre el hemisferio norte estará completamente recuperada para la década de 2030 y, en torno a 2060, el ozono se habrá rehecho por completo en todo el mundo. La desaparición gradual de los CFC tuvo también un beneficio añadido: redujo a la mitad el calentamiento global. [1]

Si hemos sido capaces de salvar la capa de ozono, también somos capaces de salvar nuestra privacidad.

La mayoría de las recomendaciones recogidas en este capítulo van dirigidas a los responsables políticos. Para poner fin a la economía de los datos —como, en su momento, para salvar la capa de ozono—, se necesita regulación. No queda más remedio. Ahora bien, lo que va a hacer que los políticos actúen es la presión que reciban de *ti* (de nosotros, de la ciudadanía). En última instancia, depende de nosotros exigir el fin del comercio de datos personales, y hay mucho que puedes hacer para contribuir a ello.

Los responsables políticos a menudo están ansiosos por protegernos. Pero pueden temer las consecuencias de tomar medidas audaces; tal vez sus colegas de partido no estén de acuerdo, tal vez los votantes no agradezcan lo que se está haciendo por su bien, tal vez la decisión que tomen perjudique sus posibilidades de ascender en el escalafón político. El poder de los políticos proviene de nosotros. Si saben que nos preocupa la privacidad y que les retiraremos nuestros votos y nuestro apoyo si no regulan la protección de nuestros datos, seguro que actuarán. Solo están esperando nuestra señal. Nuestro trabajo consiste en estar lo mejor informados que podamos para saber qué pedir a nuestros políticos. Puedes expresar tus convicciones poniéndote en contacto con tus representantes, votando y protegiendo tu privacidad por tu cuenta, que será el tema del próximo (y último) capítulo.

PONER FIN A LA PUBLICIDAD PERSONALIZADA

Volvamos a nuestro punto de partida. El origen de los aspectos más oscuros de la economía de los datos está en el desarrollo de la publicidad personalizada, y es justamente ahí donde podemos encontrar el principio de una solución. Los anuncios microfocalizados que se basan en tu identidad y tu conducta no compensan las consecuencias negativas a las que dan lugar.

Uno de los peligros más graves de la publicidad personalizada, como vimos cuando comentamos la toxicidad de los datos personales, es la posibilidad de que corroa los procesos políticos. Quizá pienses que una solución más razonable a ese problema sería prohibir los anuncios políticos, como hizo Twitter en 2019. Sin embargo, no es fácil demarcar con nitidez qué es político y qué no. Para Twitter, un contenido político es aquel que «hace referencia a un candidato, un partido político, un cargo gubernamental elegido o designado, unas elecciones, un referéndum, una iniciativa popular sometida a plebiscito, una ley, una regulación, una directiva o un fallo judicial». ¿Qué ocurre, entonces, con los anuncios que niegan el cambio climático? ¿O con aquellos que informan a la población sobre el calentamiento global? ¿O con aquellos que critican la inmigración? ¿O con los anuncios sobre clínicas de planificación familiar? Todos ellos parecen ser contenido político y podrían estar muy estrechamente ligados a un candidato o a unas elecciones, pero no está claro ni que Twitter vaya a prohibirlos, ni que deba prohibir algunos de ellos.

Una solución mejor consistiría en prohibir de manera terminante todos los anuncios personalizados. Estos mensajes publicitarios no solo polarizan la política, sino que son mucho más invasivos de lo que la mayoría de la gente piensa. Cuando ves un anuncio personalizado, no solo quiere decir que una empresa determinada sabe más de ti que tus propios amigos. Se trata de algo mucho peor. Mientras se carga la página en tu pantalla y, en muchos casos, antes de que siquiera tengas la opción de dar (o negar) tu consentimiento a la recopilación de datos, ya hay anunciantes compitiendo entre sí —con múltiples pujas en microsegundos— por el privilegio de enseñarte su anuncio.

Ese sistema de pujas en tiempo real (RTB, por sus siglas en inglés) envía tus datos personales a los anunciantes interesados, a menudo sin que tú hayas dado permiso. Supón que Amazon obtiene esos datos y te reconoce como usuario que ha visitado su sitio web antes en busca de zapatos. Tal vez le interese pagar más que otros para incitarte a comprar calzado. Y así es como, al final, se te acaba mostrando un anuncio de zapatos de Amazon. Por desgracia, en ese proceso, es posible que se hayan enviado datos muy personales —como tu orientación sexual o tu afiliación política— a quién sabe cuántos anunciantes posibles sin

que tú lo sepas ni lo hayas consentido. Y esas compañías se terminan quedando con tus datos personales. [2]

La publicidad conductual tiene un atractivo comprensible. Los usuarios no quieren ver productos que no son de su interés. Si no necesitas un vehículo para uso agrícola, que aparezcan anuncios de tractores en tu pantalla es un fastidio. A su vez, los anunciantes no quieren desperdiciar sus recursos mostrando anuncios a personas que jamás querrán comprar su producto. Ya lo dijo John Wanamaker, empresario del comercio minorista, en el siglo XIX : «La mitad del dinero que gasto en publicidad se desperdicia; el problema es que no sé qué mitad es».

La publicidad dirigida promete resolver ambos problemas mostrando a los clientes aquello que les interesa comprar, lo que a su vez garantiza que los anunciantes solo paguen por aquellos anuncios que aumenten sus ventas. En teoría, todos salen ganando. Por desgracia, la práctica no se parece en nada a la teoría. La práctica ha normalizado la vigilancia. Ha llevado a la propagación de las noticias falsas y el *clickbait* (los «ciberanzuelos»). Ha fracturado la esfera pública y ha llegado incluso a poner en riesgo nuestros procesos democráticos. Y, por si estas externalidades negativas fueran poco, la publicidad microdirigida ni siquiera cumple sus promesas: no nos muestra lo que queremos ver y no está claro que ayude a los anunciantes a ahorrar dinero o a aumentar sus ventas.

La publicidad, en su mayor parte, es una actividad mucho menos científica de lo que cabría imaginar. Los anunciantes suelen seguir una estrategia publicitaria más por intuición que porque tengan pruebas sólidas sobre lo que va a funcionar. En algunos casos, ese enfoque intuitivo ha llevado a empresas muy relevantes a malgastar millones de dólares. [3]

No existen suficientes estudios que nos permitan evaluar con un alto grado de confianza la eficacia de la publicidad personalizada. No obstante, hay razones para pensar que los anuncios dirigidos no son tan rentables como los más optimistas esperaban. [4] Las investigaciones preliminares al respecto muestran que la publicidad que usa *cookies* no aumenta los ingresos de los anunciantes más que en un 4 por ciento, aproximadamente (es decir, solo 0,00008 dólares de incremento medio por anuncio). Y, sin embargo, los anunciantes están dispuestos a pagar mucho más por un anuncio dirigido que por otro que no lo sea. Según una investigación sobre el tema, un anuncio en línea que no use *cookies* se vende por solo un 2 por ciento del precio que cuesta ese mismo anuncio si incorpora una *cookie* . [5] «Hay una especie de pensamiento mágico en torno a la publicidad dirigida [que trata de convencernos de que] todos salimos beneficiados con ella —dice Alessandro Acquisti, profesor de la Universidad Carnegie Mellon y uno de los autores del estudio—. A primera vista, puede resultar verosímil. El problema es que, si inspeccionamos más a fondo la

cuestión, vemos que hay muy poca base para corroborar esas tesis». [6]

Si los anuncios dirigidos son mucho más caros que los que no lo son, y si el aumento de ingresos que aportan es marginal, es posible que estemos perdiendo nuestra privacidad a cambio de nada. Plataformas como Google y Facebook podrían estar lucrándose de manera indebida con la venta de humo. [7] Una encuesta realizada por Digiday confirma esa sospecha. De los cuarenta ejecutivos de empresas editoras que participaron en la encuesta, un 45 por ciento respondió que la segmentación publicitaria basada en el comportamiento de los usuarios no había generado ningún beneficio apreciable, mientras que un 23 por ciento de los encuestados dijo que había hecho que sus ingresos por publicidad descendieran. [8] Como respuesta a la entrada en vigor del Reglamento General de Protección de Datos (RGPD), *The New York Times* bloqueó los anuncios personalizados y, pese a ello, no registró una caída de sus ingresos por publicidad, sino todo lo contrario, estos aumentaron. [9]

Una de las razones por las que los anuncios dirigidos pueden no ser tan eficaces para incrementar los ingresos es que la gente los detesta. [10] ¿Te acuerdas de cuando los anuncios eran creativos e ingeniosos? Eran lo bastante interesantes para que las cadenas televisivas emitieran una selección de ellos en formato de programas de una hora y la audiencia quisiera verlos. Ya no. La mayoría de los anuncios actuales —sobre todo los que se publican en línea— son desagradables, en el mejor de los casos, y aborrecibles, en el peor. Por lo general, son feos, molestos e intrusivos. La publicidad contemporánea ha olvidado las lecciones de David Ogilvy, el que para muchos fue el padre del sector, quien escribió en su día que «no se puede convencer a la gente de que compre tu producto *aburriéndola* ; solo puedes conseguirlo *despertando su interés* por comprarlo». Tampoco se puede (ni se debe) *intimidar* a la gente para que compre tu producto: «Es más fácil venderle algo a una persona dándole un amistoso apretón de manos que golpeándola en la cabeza con un martillo. Debes intentar *encandilar* al consumidor», escribió Ogilvy. [11] En muchos sentidos, los anuncios en línea son peores que un martillazo.

Una posible razón por la que las personas detestamos los anuncios dirigidos es que invaden nuestra privacidad. ¿Te has sentido alguna vez incómodamente observado por los anuncios que te aparecen? Hablas con un amigo de un tema delicado —quizá estés pensando en cambiar de trabajo, o en tener un bebé, o en comprarte una casa— y el siguiente anuncio que ves guarda relación directa con esa conversación previa que tú creías que había sido privada. No es de extrañar que los estudios indiquen que los anuncios son menos efectivos cuando la gente se inquieta por haberlos recibido. [12] Si los destinatarios saben que un anuncio los seleccionó porque los rastreó a través de la web, o porque realizó inferencias

sobre ellos, es menos probable que se dejen seducir por él.

Hace tiempo que Google intuyó que la gente no agradecería que la espiaran y adoptó un enfoque más sigiloso, como ya se ha explicado antes. ¿Recuerdas la primera vez que empezaste a entender cómo estaban usando tus datos las grandes compañías tecnológicas? Sospecho que no te enteraste porque alguna de las grandes plataformas te enviara un mensaje claro al respecto. Quizá empezaste a notar, más bien, que los anuncios que veías estaban relacionados contigo y que eran distintos de los que veían tus amigos y familiares. O tal vez leíste sobre el asunto en algún reportaje o en un libro.

El que la publicidad dirigida pueda no estar proporcionando las ventajas que se pensaba que aportaría hace que nuestra pérdida de privacidad parezca aún más inútil y absurda. Pero incluso en el caso de que los anuncios dirigidos lograran mostrarnos justo aquello que queremos ver y sirvieran para aumentar los ingresos de los comerciantes, seguiríamos teniendo muy buenos motivos para desecharlos.

Y es que los anuncios dirigidos tal vez no funcionen muy bien en el ámbito comercial, pero sí podrían ser bastante efectivos como mecanismo con el que influir en unas elecciones, como ya hemos visto. Un efecto de un 4 por ciento en las ventas de un producto no será suficiente para compensar el coste del anuncio, pero ese mismo efecto en términos de porcentaje de votos podría servir para decidir unos comicios.

Los anuncios personalizados han normalizado ciertos usos hostiles de las nuevas tecnologías. Han convertido el *marketing* en un arma de difusión de desinformación y han fragmentado y polarizado el espacio público. Mientras plataformas como Facebook recurran a la publicidad personalizada, seguirán siendo foros divisivos porque nos exponen a contenidos que nos enfrentan unos a otros, por mucho que la declaración de objetivos de la compañía diga que su misión es «crear comunidades y hacer del mundo un lugar más conectado». Facebook será perjudicial mientras siga siendo tan dominante en el ámbito de la publicidad digital.

Facebook hace que los editores serios se alejen de sus propios canales de distribución, al tiempo que fomenta los contenidos de *clickbait* . Ese debilitamiento de la relación entre los editores y sus públicos es especialmente preocupante en el caso de los periódicos, pues los obliga a depender de unas plataformas que pueden cambiar de algoritmo en cualquier momento y perjudicar su visibilidad. [13] Antes incluso de que Facebook anunciara que introduciría una modificación en su algoritmo en 2018 para favorecer las publicaciones de familiares y amigos por encima del contenido producido por los editores, los medios informativos ya estaban registrando una caída en su

tráfico referido desde Facebook. Algunos de esos sitios habían informado de descensos de hasta el 40 por ciento. BuzzFeed tuvo que despedir a personal, y el periódico más leído en Brasil, *Folha de S. Paulo* , decidió retirar su contenido de Facebook. [14]

Prohibir la publicidad dirigida potenciaría la competencia. Uno de los elementos que está impidiendo a muchos competir con Facebook y Google es la cantidad de datos personales que esas dos empresas han acaparado. Todo el mundo quiere anunciarse a través de ellas, en parte porque se supone que, cuantos más datos tenga una plataforma, más eficaz será personalizando anuncios. Si todas las plataformas utilizaran publicidad contextual, competirían en condiciones de mayor igualdad. [15] La publicidad contextual te muestra anuncios de calzado cuando escribes «zapatos» en una búsqueda. No necesita saber quién eres ni dónde has estado. Si a las empresas no se les permitiera usar datos personales para sus anuncios, se eliminaría parte de la ventaja competitiva de la que actualmente disfrutan Google y Facebook, si bien estos dos gigantes tecnológicos continuarían siendo colosos publicitarios por su enorme volumen de usuarios.

Hay un espacio para la publicidad en el mundo digital, sobre todo para la de tipo informativo (frente a la de carácter combativo o persuasivo), que es aquella que, según David Ogilvy, representa la forma de *marketing* más moral y más rentable. Los anunciantes en línea harían bien en recordar el siguiente aforismo de Ogilvy: «La publicidad es un negocio de *palabras* ». Tal vez los anuncios en línea deberían parecerse más a los de las revistas y la televisión. En vez de diseñar mensajes nocivos que nos vigilan y que distraen nuestra atención con imágenes llamativas que saltan en nuestra pantalla, se podría intentar que los anuncios en línea se basaran en hechos y palabras, siguiendo el ideal de Ogilvy. Incluir datos de un producto, en vez de adjetivos, y añadir algún buen consejo —sobre cómo quitar una mancha o cómo preparar una receta de cocina, según el artículo anunciado— son ejemplos de buenas prácticas. [16] Los anunciantes en línea deberían ofrecernos información, en vez de quitárnosla.

Los anuncios están especialmente justificados en el caso de nuevos productos y marcas; pero no hace falta que violen nuestro derecho a la privacidad para ser eficaces. Además, se puede defender la necesidad de limitar la cuota de la economía que se dedica a la publicidad. En estos momentos, los anuncios son el meollo de la economía de los datos. Sin embargo, esta excesiva presencia de los anuncios en nuestro panorama actual podría ser negativa para el bienestar general.

Un estudio reciente de aproximadamente un millón de ciudadanos europeos de veintisiete países a lo largo de tres décadas sugiere que existe una correlación

entre el aumento del gasto dedicado a publicidad en un país y el descenso del nivel de satisfacción vital. Incluso después de tener en cuenta otras variables macroeconómicas como el desempleo y las características socioeconómicas individuales, los investigadores calculan que, al duplicarse el gasto dedicado a publicidad en un país, se aprecia una caída media subsiguiente de un 3 por ciento en la satisfacción declarada por su población (un efecto equivalente a una cuarta parte del que tiene el desempleo). [17] Si la publicidad está impulsando nuestra economía a costa de nuestra felicidad, igual nos lo tendríamos que pensar dos veces al valorar la posición que le damos en nuestras vidas.

Según un informe encargado por la Asociación Nacional de Anunciantes y la Coalición de Publicidad, esta representó un 19 por ciento del producto económico total estadounidense en 2014. [18] Para ponerlo en perspectiva, el turismo aportó un 7,7 por ciento ese mismo año. [19] El valor del mercado publicitario estadounidense supera al del sector bancario. [20] Y, sin embargo, se trata de una industria que nos hace infelices. Al igual que a Jeff Hammerbacher, antiguo científico de datos de Facebook, a mí también me resulta deprimente que «las mejores mentes de [nuestra] generación estén pensando en cómo conseguir que la gente haga clic en los anuncios». [21]

Limitar los anuncios sería también una forma natural de frenar el poder de las grandes plataformas tecnológicas que tanto dependen de ellos. No olvidemos que la publicidad representa la mayor parte de los ingresos de Alphabet y de Facebook. [22]

Hay que parar a los anuncios personalizados. Deberíamos prohibir las pujas por estos en tiempo real. Deberíamos limitar la preponderancia de los anuncios o, cuando menos, incluir modificaciones para que no tengan un efecto negativo en el bienestar de las personas. Afortunadamente, no tienes que quedarte esperando a que los responsables políticos reformen el sector publicitario; puedes usar bloqueadores de anuncios (ver detalles en el capítulo siguiente).

PONER FIN AL COMERCIO DE DATOS PERSONALES

Los datos personales no deben ser algo que se pueda comprar, vender o compartir para explotarlos con fines de lucro. Las oportunidades de que se produzcan abusos son demasiadas y no dejan de proliferar. Cuanto más sensibles sean los datos, más estricta debe ser la prohibición y más severa tendría que ser la penalización por infringir esa ley. Es repugnante que ahora mismo permitamos que haya empresas que se enriquezcan con la información de que un ciudadano particular tiene una enfermedad, o de que ha perdido a su hijo en un accidente de

tráfico, o de que ha sido víctima de una violación.

No me he encontrado con ningún buen argumento que justifique la existencia de los brókeres de datos. Los brókeres de datos son los carroñeros del paisaje digital. Viven de los rastros de datos que vamos dejando, se los venden al mejor postor y rara vez muestran consideración alguna por las personas con cuya información se están lucrando.

Hace veinte años, Amy Boyer murió asesinada por un acosador después de que este hubiese comprado información personal y datos de ubicación sobre ella a Docusearch, [23] un bróker de datos que, por increíble que parezca, todavía está activo. En su sitio web, dice estar «en línea y contar con la confianza de los clientes desde hace más de veinte años». Los buitres de datos no son de fiar. Estos brókeres han vendido datos de personas a defraudadores. En 2014, LeapLab, un bróker de datos con sede en Nevada, vendió detalles íntimos de la vida de cientos de miles de personas a una «compañía» que usó esos historiales para efectuar retiradas de efectivo no autorizadas de las cuentas bancarias de esos individuos. [24] ¿Alguna vez te ha desaparecido dinero de la cuenta? Posiblemente debas agradecérselo a algún bróker de datos; es posible que vendiera (o perdiera) ese tipo de información sobre ti. La ya comentada filtración de datos sufrida por Equifax es una de las peores de la historia del mundo empresarial. [25] El que las tragedias relacionadas con los datos hayan sido relativamente pocas hasta el momento —en vista, sobre todo, de la extendida desatención a la seguridad de los datos— es un testimonio de que los seres humanos, en general, cumplimos con la ley y somos decentes. Aun así, no podemos estar siempre a expensas de la bondad de las personas. Necesitamos mejores medidas de seguridad.

La mera existencia de ficheros sensibles sobre usuarios de internet es un riesgo para el conjunto de la población. Muchas veces, los datos personales en poder de los brókeres ni siquiera están encriptados o bien protegidos. Actualmente, estos brókeres carecen de incentivos suficientes para invertir en una buena seguridad. Los gobiernos extranjeros y otros agentes malintencionados pueden jaquear esos datos y usar ese conocimiento contra nosotros. Cuantos más detalles personales nuestros recopilan los brókeres de datos, y cuantas más son las empresas nuevas a las que venden esos ficheros, más crece nuestro riesgo de salir perjudicados por un mal uso de esos datos. ¿Y qué obtenemos a cambio? Nada. ¿Acaso habíamos bebido de más cuando aceptamos este acuerdo? No. Simplemente, nunca nos preguntaron.

Comprar perfiles a los brókeres de datos ni siquiera es caro. Se puede adquirir un número de cuenta corriente por poco más de 40 céntimos de euro, y un informe completo sobre una persona puede salir por solo 85 céntimos. [26] Por

poco más de 20 euros al mes, puedes comprobar los antecedentes de todos tus conocidos (pero, por favor, no lo hagas). En mayo de 2017, Tactical Tech y la artista Joana Moll adquirieron un millón de perfiles individuales de USDate, un bróker de datos sobre sitios de citas en línea. En el lote iban incluidos casi 5 millones de fotografías, nombres de usuario, direcciones de correo electrónico, detalles sobre la nacionalidad, el género y la orientación sexual, rasgos de personalidad, etcétera. Aunque existe alguna que otra duda a propósito de la fuente original de los datos, hay indicios que dan a entender que procedían de algunas de las plataformas de citas más populares. Les costaron 136 euros (unos 161 dólares). [27] Que una transacción así sea siquiera posible es asombroso. Y una barbaridad. Que los datos personales sean tan *valiosos* y tan *baratos* al mismo tiempo es la peor combinación posible para la privacidad.

Parte del trabajo de la buena regulación es lograr impedir que un tipo determinado de poder se transforme en otro tipo. Por ejemplo, una buena regulación es aquella que evita que el poder económico se convierta en poder político (esto es, que el dinero compre votos o la voluntad de los políticos). En el caso que aquí nos ocupa, lo que se necesita es impedir que el poder acumulado a través de los datos personales se transforme en un poder económico o político. Los datos personales deberían servir para beneficiar a los ciudadanos, no para llenar los bolsillos de los buitres de datos.

Incluso en la más capitalista de las sociedades estamos de acuerdo en que hay ciertas cosas que no están a la venta; entre ellas están las personas, los votos, los órganos humanos y los resultados deportivos. A esa lista deberíamos añadir los datos personales. «Datos personales» suena demasiado abstracto. Y esta es una abstracción muy oportuna para los buitres de datos. De lo que estamos hablando, en realidad, es de nuestras esperanzas y miedos, nuestros historiales médicos, nuestras conversaciones más privadas, nuestras amistades, nuestros más oscuros remordimientos, nuestros traumas, nuestras alegrías, de cómo suena nuestra voz y de cómo nos late el corazón cuando hacemos el amor. [28] [*] Esto es lo que se explota con fines de lucro, demasiadas veces, en contra de nuestro interés.

Prohibir el comercio de datos personales no significa prohibir la recopilación ni el uso adecuado de dichos datos. Recolectar algunos datos personales a veces es necesario. Necesitas compartir algunos con tu médico, por ejemplo, para que te pueda prestar la atención adecuada. Sin embargo, nuestro sistema sanitario no debería estar autorizado a compartir esos datos ni, menos aún, a venderlos.

Poner fin al comercio de datos personales no significa que no se puedan compartir datos de otros tipos —el veto solo debe aplicarse a los datos *personales* . De hecho, hay datos no personales que deberían ser ampliamente compartidos para facilitar la colaboración y la innovación. Tal como defienden el

informático Nigel Shadbolt y el economista Roger Hampson, la combinación correcta es tener «datos públicos abiertos» y «datos privados protegidos». [29]

Necesitamos, no obstante, contar con unas definiciones más estrictas de lo que entendemos por «datos personales». En la actualidad, normas legislativas como el Reglamento General de Protección de Datos (RGPD) no se aplican a los datos anonimizados. Sin embargo, como ya vimos en el capítulo 1, ocurre con demasiada frecuencia que datos que se creían anónimos han terminado siendo reidentificados. Parte del problema reside en que no podemos estar seguros de qué técnicas podrían desarrollarse y utilizarse en el futuro para reidentificar a individuos a partir de una base de datos «anónima». Por lo tanto, tenemos que ser todo lo rigurosos que nuestra imaginación nos permita al definir qué entendemos por «anónimo».

También necesitamos tener una idea muy amplia de aquello que entra en la categoría del «comercio de datos». Los brókeres de datos proporcionan datos personales a cambio de dinero, pero hay otras muchas empresas que realizan operaciones comerciales menos burdas con datos. Facebook, por ejemplo, ha facilitado a otras compañías acceso a datos personales de sus usuarios a cambio de que estas firmas den a Facebook un trato de favor en sus plataformas. Facebook concedió a Netflix y a Spotify capacidad para leer mensajes privados de sus usuarios, y dejó asimismo que Amazon accediera a nombres de sus usuarios y a otra información de contacto a través de los amigos de estos. Parte de lo que recibió a cambio fueron datos con los que alimentar su intrusiva herramienta de sugerencia de amigos: «Personas que quizá conozcas». [30] Los datos personales no deberían formar parte de nuestro mercado comercial. No deberían venderse, revelarse, transferirse ni compartirse por vía alguna para fines de lucro o de obtención de una ventaja comercial.

Tampoco en este caso tienes que esperar a que los responsables políticos prohíban el comercio de datos personales para empezar a hacer algo al respecto; puedes seguir los consejos del capítulo siguiente.

PONER FIN A LA RECOPILACIÓN DE DATOS PERSONALES

Algunas grandes compañías tecnológicas se hicieron grandes a base de saquear nuestros datos sin nuestro permiso, sin pensar en las posibles consecuencias de su modo de actuar para sus usuarios y para la sociedad en general. Esta actitud temeraria se refleja a la perfección en el lema interno de Facebook: «Muévete rápido y rompe cosas». La estrategia de las grandes tecnológicas ha consistido en hacer lo que les plazca hasta que se topan con alguna resistencia. Si

encuentran alguna oposición, las grandes tecnológicas suelen intentar ignorarla. Cuando esto no funciona, prueban a seducir al público ofreciendo algún nuevo beneficio adicional, e intentan agotar a sus críticos dando una retahíla de respuestas vacías. Solo cuando la resistencia se vuelve persistente, se consigue que las grandes tecnológicas den un paso atrás (después de haber dado muchos hacia delante). Lo que esperan conseguir con este ciclo es que nos vayamos aclimatando de forma progresiva y terminemos por aceptar unas condiciones que jamás habríamos aceptado si nos las hubieran planteado de golpe desde el principio. [31]

Fue a través de este ciclo como nos acostumbramos a que nuestros datos fueran recopilados de forma automática por cualquiera que dispusiera de medios para hacerlo. Lo hemos tolerado porque nos enteramos de lo que ocurría años más tarde, cuando ya estábamos enganchados a la tecnología digital, y porque se nos dijo que era necesario para que nuestros dispositivos continuaran funcionando correctamente, y que ya era una práctica empresarial generalizada. Nos contaron asimismo que necesitábamos la vigilancia por nuestra propia seguridad. Solo cuando las grandes corporaciones se enfrentaron a una reacción adversa (el ya mencionado *techlash*) y se introdujeron normativas como el RGPD, comenzaron a hacer ciertas concesiones, como la de explicarnos algo sobre la clase de datos que recolectan sobre nosotros. Pero esas pequeñas concesiones no son suficientes. Ahora estamos mejor informados. Sabemos que es posible tener tecnología puntera sin sufrir invasiones de nuestra privacidad. Y sabemos que la privacidad es un elemento importante para garantizar nuestra seguridad.

En la situación actual, la recopilación de datos es una práctica generalizada. Casi todos los sitios web, aplicaciones y dispositivos con los que interactúas recopilan tus datos. Algunas de esas compañías ni siquiera saben qué hacer con ellos. Solo los recolectan por si les fueran útiles en el futuro. La recogida de datos no es inocua. Nos pone en riesgo a todos.

Hasta el momento, la legislación se ha centrado principalmente en los *usos* de los datos, más que en su recogida. Aunque el RGPD incorpora un principio de minimización de datos, según el cual las empresas solo deberían recolectar aquella información personal que sea adecuada, relevante y necesaria, muchas organizaciones se escudan en una interpretación muy amplia de los «intereses legítimos» que tienen para procesar datos. Necesitamos ser más estrictos limitando la recopilación de datos.

Cualquiera que haya usado internet alguna vez sabe que el actual sistema de «consentimiento» de la recolección de datos es defectuoso. Sitúa una carga de responsabilidad demasiado pesada sobre los hombros de los ciudadanos. Es muy

molesto tener que hacer clic en (según los casos) decenas de casillas para rechazar la recopilación de datos; a veces, si dices «no» a las *cookies* , se te castiga a tener que repetir el mismo proceso cada vez que visitas ese sitio web. Si no existiera la recopilación de datos por defecto, la gente no tendría que estar pidiendo continuamente que se respete su privacidad. Y las personas que optaran de forma voluntaria por permitir la recolección de sus datos podrían ser recordadas de forma legítima y solo tendrían que indicarlo una vez.

La opción por defecto —para las empresas, los organismos estatales y la configuración de usuario de todos los sitios web y aplicaciones— debería ser la *no* recopilación de datos, o la recogida de solamente los mínimos *necesarios* . Las opciones por defecto importan, porque la mayoría de las personas nunca tocan las configuraciones que tienen preseleccionadas. Las personas tendrían que optar de manera verdaderamente voluntaria por la recopilación de datos, en vez de tener que indicar su negativa. La interpretación de lo que son datos «necesarios» debería ser restrictiva y ceñirse a aquellos que sean indispensables para proporcionar un servicio que interese; no para financiar ese servicio vendiendo nuestros datos o facilitando que otros accedan a nosotros, sino para construir o mantener el servicio en cuestión. Algunos servicios precisan de datos de las personas para trazar mapas del tráfico, por ejemplo, pero no necesitan datos de *todo el mundo* para cumplir esa función de forma eficaz. Si los datos de una muestra de usuarios son suficientes, cualquier recopilación que vaya más allá es innecesaria.

Tenemos que invertir más en innovación en materia de privacidad. Si las grandes empresas tecnológicas se ven obligadas a afrontar el reto de inventar formas de usar datos sin dejar de proteger la privacidad, es muy probable que estén a la altura del desafío. Si dejamos que continúen comportándose como hasta la fecha, es posible que nunca se desarrollen esas innovaciones.

Un método prometedor para la recolección de datos es la «privacidad diferencial». Esta significa básicamente la inserción del suficiente ruido matemático en una base de datos para que se pueda camuflar de forma efectiva a todos los que figuran en ella —es decir, sin que se pueda inferir nada en particular sobre ninguno de esos individuos—, pero sin impedir que se puedan extraer respuestas precisas al realizar análisis estadísticos. Puede parecer una idea compleja, pero he aquí un ejemplo sencillo para ilustrarla.

Supón que quieres saber cuántas personas residentes en Londres votaron a favor del Brexit. Normalmente, llamarías a unos miles de números de teléfono y preguntarías a cada persona qué votó en el referéndum. Aunque no tomaras nota de sus nombres, si fueras anotando los números de teléfono y el sentido del voto de cada encuestado, estos electores serían fáciles de identificar y se pondría en

riesgo su derecho al voto secreto. Sin embargo, si quisieras recoger datos aplicando la privacidad diferencial, llamarías también por teléfono a unas miles de personas, pero en vez de preguntarles directamente por lo que votaron, les pedirías que echaran una moneda al aire. Les dirías que, si les sale cara, te digan qué votaron; que, si les sale cruz, vuelvan a tirar la moneda y, entonces, si les sale cara esta segunda vez, te digan la verdad, y que, si de nuevo les sale cruz, te mientan. Lo importante, en todo caso, es que nunca te digan si les ha salido cara o cruz. Dado que ya tienes controlada la frecuencia con la que los encuestados te van a mentir, sabes que, aproximadamente, una cuarta parte de tus resultados van a ser incorrectos (mentiras), por lo que podrás realizar los ajustes estadísticos oportunos. El resultado será una base de datos que es casi igual de exacta que las bases corrientes y que no contiene ningún dato personal, porque solo los encuestados saben qué les salió al lanzar la moneda. No hay forma de saber quién votó a favor del Brexit, pero sí de conocer de forma aproximada cuántas personas votaron por esa opción. Cada participante puede dar una «negativa creíble» como respuesta; siempre podrán decir que no votaron por el Brexit y nadie podrá demostrar lo contrario (o, al menos, no a partir de esta base de datos). [32]

Desde luego, no todos los tipos de datos pueden reunirse empleando la privacidad diferencial. El método necesita ser perfeccionado para que las instituciones puedan implementarlo con facilidad y eficacia. No pretendo sugerir que la privacidad diferencial es perfecta, o que es la solución a todos nuestros problemas. No lo es. Y si no se pone en práctica de un modo adecuado, puede generar una falsa sensación de seguridad. Aun así, me sigue gustando como ejemplo porque ilustra la posibilidad de desarrollar formas creativas de analizar datos sin poner en peligro la privacidad de las personas. El cifrado homomórfico y el aprendizaje federado son otras dos técnicas que vale la pena explorar. Deberíamos invertir más en el desarrollo de herramientas de privacidad, en lugar de hacerlo solo en métodos de explotación de los datos con fines de lucro, conveniencia o eficiencia.

Siempre que no haya más alternativa que recopilar datos personales, estos solo deberían recolectarse cuando el individuo en cuestión dé su consentimiento de manera consciente y libre, y habiéndose especificado antes los usos que se dará a esos datos y la política prevista para su eliminación (sobre esto, véase más en el último apartado del capítulo). Sin embargo, limitar la recogida de datos personales no es suficiente, pues se puede obtener información sensible no solo a partir de la recopilación directa de datos, sino también a partir de inferencias.

PONER FIN A LAS INFERENCIAS SENSIBLES SUBREPTICIAS

Las organizaciones sedientas por saber más de nosotros pueden eludir los límites que les hayamos fijado si, en vez de recopilar información sensible sobre nosotros, se dedican a inferirla. Los rastros digitales que vamos dejando cuando interactuamos con la tecnología se tratan habitualmente como muestras de conducta que se usan luego para hacer inferencias sobre nosotros.

En los últimos años, han proliferado las teorías referentes a lo que nuestros rastros de datos dicen sobre nosotros. El modo en que las personas usan los teléfonos inteligentes puede utilizarse para predecir puntuaciones en ciertos tests de aptitudes cognitivas como la memoria o la concentración. Se pueden detectar problemas de memoria a partir de la rapidez con la que las personas escriben en sus teléfonos, los errores que cometen y la velocidad con la que se desplazan por su lista de contactos. [33] Se han usado los «me gusta» de Facebook, por ejemplo, para inferir la orientación sexual, el origen étnico, las ideas religiosas y políticas, los rasgos de personalidad, la inteligencia, la felicidad, el consumo de sustancias adictivas, la condición de ser hijo de padres separados, la edad y el género de las personas. [34] Se pueden usar las pautas del movimiento ocular para detectar la dislexia. El paso al que caminas, medido por el acelerómetro de tu teléfono inteligente, puede utilizarse para inferir tu esperanza de vida. Tus publicaciones en Twitter y las expresiones de tu rostro pueden usarse a su vez para descubrir una depresión. La lista continúa, pero ya te puedes hacer una idea: muchas empresas e instituciones están empleando de forma sistemática tus señales externas para inferir información privada acerca de ti. [35]

Como ocurre con la recopilación subrepticia de datos personales, preocupa que tu privacidad pueda ser violada sin que te enteres. Peor aún, en el caso de las inferencias, tienes muy escaso o nulo control sobre algunas de esas señales externas que vas dejando, por lo que no hay mucho que puedas hacer para protegerte. Puedes intentar no regalar tus datos personales, pero no puedes cambiar tu cara ni tu manera de caminar, por ejemplo, ni empezar a escribir de forma diferente en tu teléfono. Todos estos son marcadores involuntarios. Y no tienes manera de saber si alguien está usando esa información ni con qué fines.

Otro tema preocupante relacionado con las inferencias sensibles es que pueden equivocarse contigo y, pese a ello, ser usadas contra ti. Las inferencias basadas en algoritmos son probabilísticas y, como tales, solo aciertan algunas veces. La precisión de las inferencias varía considerablemente, y las empresas a menudo no tienen incentivos para asegurarse de que sean lo más precisas posibles. Mientras las empresas consideren que las inferencias les proporcionan alguna ventaja, pueden contentarse con usarlas tal cual, aunque sean muy

imperfectas.

Unos investigadores, por ejemplo, lograron inferir correctamente en un 73 por ciento de los casos si una persona era fumadora a partir de sus «me gusta» en Facebook. [36] Supón que una empresa utiliza esta inferencia como filtro para contratar empleados. Si tiene suficientes candidatos para cubrir un puesto, es posible que no le importe equivocarse en un 27 por ciento de esos solicitantes, pues, desde su punto de vista, sigue siéndole más ventajoso disponer de esa información. Sin embargo, si tú eres una de las desafortunadas personas a las que han clasificado erróneamente como fumadora, habrás sufrido una injusticia sin que llegues a enterarte nunca de ello, porque es muy probable que la empresa nunca te explique por qué no te dieron el puesto.

Las inferencias sensibles pueden ser aceptables en según qué casos. Tal vez seas un paciente que quiera que tu médico analice cómo escribes en tu teléfono inteligente para que pueda detectar algún problema cognitivo lo antes posible. Sin embargo, las inferencias sensibles tienen que regularse con igual rigor que los datos personales, ya que se usan como si fueran estos, incluso cuando son erróneas. A los ciudadanos se les debería pedir consentimiento antes de usar sus señales externas para inferir información privada sobre ellos. Deberíamos el poder de impugnar y rectificar las inferencias incorrectas, y la información sensible inferida debería recibir el mismo tratamiento que los datos personales.

Una vez abolidos los anuncios microdirigidos, la compraventa de datos personales, la recopilación datos personales por defecto y las inferencias sensibles, las perspectivas de la privacidad mejorarían muchísimo. Aun así, esas medidas no bastarían todavía por sí solas, pues aún nos quedaría pendiente ocuparnos de los contextos en los que los datos personales no se venden pero pueden utilizarse en contra de los intereses de los ciudadanos.

IMPONER RESPONSABILIDADES FIDUCIARIAS

En la mayoría de los países, la ley no impone a los sospechosos de un delito a autoincriminarse. Hay algo perverso en hacer que las personas sean cómplices de su propia caída. En California, un juez federal prohibió a la policía obligar a los sospechosos a que abrieran sus teléfonos móviles porque lo consideró un gesto análogo a una autoincriminación. [37] Y, sin embargo, toleramos que inocentes ciudadanos de la red sean forzados a entregar sus datos personales para que luego se dé a esa información toda clase de usos contrarios a sus intereses. Deberíamos proteger a estos ciudadanos, al menos tanto como protegemos a los sospechosos de un delito. Nuestros datos personales no deberían usarse contra

nosotros.

Para lograr este objetivo, deberíamos someter a las instituciones y organizaciones que recogen y gestionan datos personales a unas estrictas responsabilidades fiduciarias. [38] Las figuras fiduciarias, como pueden ser los asesores financieros, los médicos o los abogados, tienen un deber de lealtad y cuidado con sus clientes: el mismo deber que tendrían que tener las empresas que poseen nuestros datos personales.

La palabra «fiduciario» proviene del verbo latino *fidere* , confiar. La confianza es la esencia de las relaciones fiduciarias. En primer lugar, porque a un fiduciario se le confía algo que es muy valioso (tus finanzas, tu cuerpo, tus asuntos legales o tus datos personales). En segundo lugar, porque al confiar ese bien valioso a otros, te vuelves muy vulnerable ante ellos. Al aceptar lo que les confías y al reconocer así la vulnerabilidad que te vincula a ellos, los fiduciarios adquieren una deuda de confianza contigo. [39]

Las responsabilidades fiduciarias protegen a los individuos que se encuentran en una posición de debilidad frente a profesionales que se supone que deben servirlos, pero que podrían tener un conflicto de intereses. Tu asesora financiera podría hacer demasiadas operaciones con tu cuenta solo para cobrar más comisiones, o podría utilizar tu dinero para comprarse títulos para sí. Tu médico podría practicarte una cirugía arriesgada o innecesaria solo por su interés en aprender o en añadir un caso más a una investigación para un artículo académico. Tu abogada podría vender tus secretos a otro cliente con intereses contrapuestos a los tuyos. Y, como ya hemos visto, quienes recopilan tus datos podrían dárselos a buitres de datos, delincuentes, etcétera. Ninguno de esos profesionales debería abusar del poder que se les ha concedido en virtud de su profesión.

Las responsabilidades fiduciarias, en resumen, son oportunas cuando existe una relación económica en la que se observa una asimetría de poder y conocimiento, y en la que un profesional o una empresa puede tener intereses en conflicto con los de sus clientes. Los asesores financieros, los médicos, los abogados y los expertos en datos saben mucho más, respectivamente, de finanzas, medicina, derecho y datos que tú. Tu asesora financiera probablemente entiende mucho más que tú de tus riesgos financieros. Tu médico comprende mejor que tú lo que está pasando en tu organismo. Tu abogada conoce más a fondo tu problema legal que tú. Y quienes analizan tus datos podrían saber (o podrían creer que saben) mucho más sobre tus costumbres y sobre tu psicología que tú. Ese conocimiento no debería usarse en tu contra.

Los fiduciarios deben actuar en beneficio de sus clientes y, si surgen conflictos, anteponer los intereses de los clientes a los suyos. Las personas que

no quieran asumir responsabilidades fiduciarias no deberían aceptar que se les confíe información o activos personales de valor. Si no quieres tener el deber de actuar conforme al interés de tus pacientes, no seas médico. No basta con tener ganas de practicar intervenciones médicas en los cuerpos de otras personas. La profesión conlleva ciertas expectativas éticas. De la misma forma, si una empresa no quiere hacer frente a responsabilidades fiduciarias sobre los datos personales, tampoco debería dedicarse a recopilar esos datos. Querer analizar esa clase de información con fines comerciales o de investigación está muy bien, pero es un privilegio que conlleva responsabilidades.

Quienes critican la idea de que las responsabilidades fiduciarias deberían aplicarse también a las grandes compañías tecnológicas apuntan a que una política así entraría en contradicción con las responsabilidades que esas compañías tienen con sus accionistas. Según la legislación vigente en Delaware —donde están constituidas Facebook, Google y Twitter—, los directores están obligados «a tener el bienestar del accionista como único objetivo y a considerar otros intereses solo en la medida en que tal consideración esté relacionada de un modo razonable con el bienestar del accionista». [40]

Que las compañías deban esforzarse únicamente por beneficiar a sus accionistas, aun en detrimento de sus clientes, parece una política moralmente cuestionable, sobre todo si la actividad de la empresa en cuestión tiene efectos negativos en la vida de millones de ciudadanos. Moralmente, los intereses económicos de los accionistas no pueden prevalecer sobre los derechos de privacidad ni sobre los intereses democráticos de los miles de millones de usuarios de las grandes tecnológicas. Una opción para solucionar este problema sería instaurar una regla mediante la cual, siempre que los intereses de los accionistas choquen con los de los usuarios, sean prioritarias las responsabilidades fiduciarias para con los usuarios. Otra opción consistiría en imponer multas suficientemente elevadas a las empresas que incumplan sus responsabilidades fiduciarias respecto de sus usuarios, de tal manera que también a los accionistas les interese que esas compañías cumplan con tales deberes con el fin de no perjudicar sus ingresos.

Las responsabilidades fiduciarias ayudarían mucho a que los intereses de las grandes compañías tecnológicas se alinearan con los de sus usuarios. Si las empresas tecnológicas quieren arriesgar nuestros datos, tendrían que arriesgar su negocio en el proceso. Mientras las empresas tecnológicas puedan arriesgar nuestros datos sabiendo que nosotros seremos los únicos que pagaremos la factura —en forma de exposición de nuestra intimidad, robos de identidad, extorsiones, discriminaciones injustas, etcétera—, seguirán actuando sin cuidado.

Añadiendo las responsabilidades fiduciarias a la lista, el paisaje de los datos queda muy mejorado. Nuestros datos ya no se compartirían, ni se venderían, ni se usarían contra nosotros. No obstante, nuestros datos personales todavía podrían perderse por negligencia, por lo que es necesario tener estándares de ciberseguridad más elevados.

MEJORAR LOS ESTÁNDARES DE CIBERSEGURIDAD

Nuestra privacidad no estará protegida de forma adecuada mientras las apps, los sitios web y los dispositivos con los que interactuamos sean inseguros. Es demasiado fácil robar datos. Tal y como están las cosas ahora, las compañías no están motivadas para invertir en ciberseguridad, pues esta, además de ser cara, no suele ser apreciada por los usuarios porque es invisible. Los ciudadanos de la red no disponen de una manera fácil de comparar los estándares de seguridad de los diferentes productos. [41] Sabemos más o menos qué aspecto tiene una puerta segura, pero no qué señales pueden indicarnos una seguridad comparable cuando hablamos de aplicaciones o de sitios web.

Las empresas no solo no tienen mucho que ganar invirtiendo en ciberseguridad, sino que no tienen suficiente que perder si las cosas fallan. Si se produce un robo de datos, los clientes son quienes se llevan la peor parte. Si se considera que una compañía ha cometido una negligencia grave, puede ser sancionada, pero, si la multa no es lo bastante grande (por ejemplo, si no supera el importe de lo que habría costado invertir en ciberseguridad), las empresas considerarán tales sanciones como un coste asumible de su operación comercial.

La ciberseguridad es un problema de acción colectiva. La sociedad estaría mejor si todos invirtieran en unos estándares de ciberseguridad aceptables. Los secretos de las organizaciones estarían mejor protegidos y estas podrían disfrutar de una mayor confianza por parte de sus clientes. Los datos de los ciudadanos estarían seguros. Y la seguridad nacional también estaría mejor salvaguardada. Sin embargo, a la mayoría de las empresas no les interesa invertir en seguridad porque es una inversión cara que les reporta muy escasas ventajas, y eso puede ponerlas en desventaja con respecto a sus competidores. En la situación actual, los productos inseguros pueden expulsar del mercado a los productos seguros, porque invertir en ciberseguridad no sale rentable.

La regulación gubernamental es la forma de mejorar la seguridad. Si no fuera por las normativas gubernamentales, los edificios, los fármacos, los alimentos, los automóviles y los aviones serían mucho menos seguros de lo que lo son. Las compañías tienden a quejarse cuando se las obliga por primera vez a mejorar sus

estándares de seguridad. Es bien conocido que las automovilísticas se opusieron inicialmente a la instalación de los cinturones de seguridad obligatorios. Les parecía que eran feos y que los usuarios los detestarían. Lo cierto era que los usuarios estaban encantados de poder viajar más seguros. Con el tiempo, las empresas terminan por aceptar esas regulaciones que las protegen a ellas y también a sus clientes de desastres devastadores para la seguridad. Y acaban entendiendo que la regulación a veces es la única manera de hacer que una compañía invierta en algo valioso, cuando esto no es inmediatamente rentable, sin tener que incurrir en una desventaja competitiva, porque la competencia tiene que hacer lo mismo.

Aunque buena parte de las pérdidas de privacidad que hemos padecido desde 2001 han sido consecuencia directa o indirecta de la supuesta priorización de la seguridad por parte de los gobiernos, la experiencia nos ha enseñado que la seguridad y la privacidad no componen un juego de suma cero. Cuando erosionamos nuestra privacidad, lo más habitual es que debilitemos también nuestra seguridad. Se ha permitido que internet sea una esfera insegura para que las empresas y los gobiernos sean capaces de arrebatarnos nuestros datos con el (teórico) fin de preservar nuestra seguridad. La realidad es que un internet inseguro es extremadamente peligroso, tanto para los individuos como para las compañías y las sociedades.

Si nuestros dispositivos no son seguros, los regímenes hostiles pueden aprovecharlos para espiar a los altos cargos de nuestro Gobierno. Agentes adversarios podrían derribar la red eléctrica de todo un país jaqueando unas decenas de miles de aparatos de elevado consumo, como calentadores de agua o aires acondicionados, y provocando un fuerte pico en la demanda de electricidad. [42] También podrían hacerse con el control de centrales nucleares, [43] o incluso de armas atómicas. [44] Un ciberataque a gran escala podría paralizar a todo un país. [45] Es una de las dos amenazas catastróficas más destacadas que los gobiernos mundiales tienen identificadas en sus registros de riesgos. La otra es una pandemia.

Los expertos llevan *décadas* avisando del riesgo de las pandemias. Y, aun así, no solo las sociedades han seguido insistiendo en las arriesgadas prácticas que sabemos que pueden provocar pandemias (como, por ejemplo, los mercados de animales vivos o la ganadería intensiva), sino que ni siquiera nos hemos preparado para enfrentarlas. La pandemia de coronavirus nos sorprendió, por ejemplo, sin suficiente material protector para los profesionales sanitarios (algo imperdonable, dado lo que sabíamos). Los seres humanos podemos prevenir aquello que no hemos experimentado con anterioridad, pero no nos resulta fácil hacerlo. Usar nuestra imaginación para prever lo que puede salir mal es

fundamental para motivarnos a actuar.

Imagínate lo que sería estar en una situación de confinamiento y que tu país sufriera un ciberataque a gran escala. Internet se colapsa. Puede que el servicio eléctrico también. Y hasta tu línea telefónica fija, si es que todavía tienes una. No puedes contactar con tu familia, ni llamar a tu médico, ni tan siquiera acceder a las noticias. No puedes salir por culpa de la pandemia. Oscurece temprano y solamente te queda una vela (¿quién guarda cajas de velas a estas alturas?). Tu calefacción eléctrica no funciona. No sabes qué ha ocurrido, ni cuándo volverá la normalidad.

No es un escenario tan inverosímil. A fin de cuentas, los ciberataques han alcanzado niveles máximos a raíz de la pandemia de coronavirus. [46] Con tanta gente trabajando desde casa con una wifi poco segura y unos dispositivos mal protegidos también, la «superficie de ataque» (los puntos de entrada posibles) aumentó. La entidad administradora del sistema de distribución de electricidad de Gran Bretaña fue blanco de un ciberataque durante el confinamiento; por suerte, no llegó a afectar al suministro eléctrico. [47] Los ataques contra la Organización Mundial de la Salud (OMS) se quintuplicaron durante ese mismo periodo. [48] Es solo cuestión de tiempo antes de que se produzca un ciberataque masivo. Lo sabemos, igual que sabíamos que, tarde o temprano, se produciría una pandemia. Tenemos que estar mejor preparados y tenemos que actuar ahora si queremos contar con una mínima posibilidad de impedirlo o mitigarlo.

Para mejorar nuestra ciberseguridad, será crucial que desconectemos sistemas. [49] La tendencia actual es que todo esté interconectado: tus altavoces y tu teléfono, tu teléfono y tu ordenador, tu ordenador y tu televisor, etcétera. Si los entusiastas de las tecnologías se salieran con la suya, el siguiente punto de conexión sería tu cerebro. Es una mala idea. Usamos puertas cortafuegos para contener la extensión de un potencial incendio en nuestra casa o en nuestro edificio, y también fabricamos nuestros barcos con varios compartimentos estancos para limitar el alcance de una potencial entrada de agua. Necesitamos crear separaciones análogas en el ciberespacio. Cada nueva conexión en un sistema es un punto de posible entrada. Si todos tus dispositivos están conectados, eso quiere decir que los jáqueres podrían acceder a tu teléfono (un aparato relativamente sofisticado, sensible y seguro, suponiendo que sea un buen móvil) a través de tu cafetera inteligente (que, muy probablemente, es un sistema inseguro). Si todos nuestros sistemas nacionales están igualmente interconectados, un ciberataque podría hacerlos caer a todos.

En un principio, la mejora de los estándares de ciberseguridad pasará sobre todo por parchear los sistemas poco seguros. Con el tiempo, sin embargo, la seguridad tendrá que hornearse en el diseño de las tecnologías. En la actualidad,

por ejemplo, la autentificación en los protocolos de conexión entre tu teléfono inteligente y las torres de telefonía a las que se conecta es inadecuada. Tu móvil va cediendo datos sensibles a todas esas antenas de la red. Por eso los receptores IMSI pueden aspirarte los datos, como vimos en el capítulo 1. [50] Tenemos que empezar a diseñar toda la tecnología pensando en cómo protegerla de posibles jáqueres. La época en que internet podía parecerse a una casa en el campo, sin vallas, puertas ni cerraduras, se terminó hace años. Tenemos que ponernos al día con la realidad.

BORRAR DATOS

Sin más anuncios personales, buitres de datos ni recopilación de datos por defecto, y con responsabilidades fiduciarias y una ciberseguridad fuertes, habríamos logrado reconstruir buena parte de un ecosistema favorable a nuestra privacidad. Pero ¿qué pasa con todos los datos personales que nos han arrebatado en el pasado, y con aquellos otros que se recolectarán legítimamente en el futuro? Tenemos que borrar los datos personales que se hayan recopilado de forma subrepticia e ilegítima. Incluso en el caso de datos personales recogidos por vías justificadas y con fines necesarios, siempre debería haber un plan previsto para su borrado. Salvo en contadas excepciones (como los registros de nacimientos), no debería recopilarse dato alguno sin asegurarse antes de que existirá la posibilidad de borrarlo y sin un plan previo para eliminarlos.

En su libro *Delete* , Viktor Mayer-Schönberger sostiene que en la era digital deberíamos rescatar la virtud de olvidar. La capacidad de olvidar es un componente importante de una vida sana. Imagina que no fueras capaz de olvidar nada de lo que has vivido. Unos investigadores estudiaron el caso de Jill Price, una californiana que carece del don de olvidar sus experiencias. Fue capaz, por ejemplo, de recordar al instante lo que había hecho todas las Semanas Santas desde 1980 a 2008. Así, sin previo aviso ni preparación. Su memoria es de tal riqueza que eclipsa su presente. No le ha traído ni felicidad ni éxito profesional. Es una persona relativamente normal que se siente ansiosa y sola en compañía de sus rebosantes recuerdos.

El psicólogo cognitivo Gary Marcus defiende la hipótesis de que la extraordinaria memoria de Price podría no deberse a que posea un cerebro inusual, sino más bien a un trastorno obsesivo-compulsivo que no le permite desprenderse del pasado. [51] Tener registros permanentes por defecto podría estar recreando en todos nosotros esa especie de obsesión, o al menos algunas de sus características negativas.

Las personas que recuerdan demasiado desearían poder desactivar (en ocasiones, al menos) una capacidad que puede experimentarse como una maldición. Cuando tu mente se aferra al pasado, cuesta avanzar, dejar atrás momentos más trágicos y más felices, y vivir en el presente. Resulta difícil aceptar lo que tienes delante si el tirón de todos esos tiempos mejores y peores se siente tan vivo todavía. Los peores momentos pueden entristecerte, y los mejores, inspirarte nostalgia. Rememorar de forma constante lo que otros hayan dicho y hecho también puede convertirte en una persona prisionera del resentimiento.

Olvidar no solo es una virtud de los individuos, sino también de las sociedades. El olvido social proporciona segundas oportunidades. Eliminar antiguos antecedentes penales de delitos menores o juveniles, olvidar bancarrotas y borrar los registros de las deudas pagadas ofrecen una segunda oportunidad a las personas que han cometido errores. Las sociedades que lo recuerdan todo tienden a ser impías.

Nunca hemos recordado tanto como hoy, como individuos y como sociedades. Antes de la llegada de los ordenadores, teníamos dos formas de olvidar: una voluntaria —quemando o destruyendo nuestros registros e historiales—, y otra involuntaria, ya que al no disponer de capacidad para dejar constancia de la mayoría de los acontecimientos, nos olvidábamos de ellos de manera natural, o perdíamos nuestros registros por culpa de accidentes o por simple deterioro físico de sus soportes.

Durante la mayor parte de la historia, mantener registros ha sido difícil y costoso. El papel solía ser muy caro y se necesitaba mucho espacio para almacenarlo. Escribir requería tiempo y dedicación. Esas limitaciones nos obligaban a elegir lo que queríamos recordar. Solo una mínima parte de lo ocurrido llegaba a preservarse y, aun en esos casos, la memoria era más efímera de lo que es hoy; cuando el papel que se usaba no estaba libre de ácido, por ejemplo, se desintegraba con bastante rapidez. Esos documentos tenían una fecha de caducidad intrínseca fijada por los materiales de los que estaban hechos. [52]

La era digital ha transformado por completo la economía de la memoria. En la actualidad, es más fácil y barato recordarlo todo que olvidarlo. Según Mayer-Schönberger, hay cuatro elementos tecnológicos que han contribuido a que recordar se haya convertido en la opción por defecto: la digitalización, el bajo coste del almacenamiento, la facilidad de recuperación y el alcance mundial. Las experiencias se transforman automáticamente en datos informáticos que se guardan en dispositivos de almacenaje cada vez más reducidos y baratos. Luego accedemos a nuestros datos tras teclear unas pocas letras y, con un solo clic, los

enviamos a cualquier parte del planeta.

Desde el momento en que la recolección de datos se automatizó y su almacenamiento se abarató hasta tal punto que se volvió realista aspirar a recolectarlo todo, pasamos de tener que seleccionar qué recordar a tener que escoger qué olvidar. Y como seleccionar requiere un esfuerzo, olvidar se ha vuelto más caro que recordar por defecto.

Es fácil que nos sintamos tentados a pensar que tener más datos nos hará necesariamente más inteligentes, o nos capacitará para tomar mejores decisiones. La realidad, sin embargo, es que puede obstaculizar nuestras aptitudes para pensar y decidir. El olvido humano representa, en parte, un proceso activo de filtrado de lo que es importante. No seleccionar aquello que recordamos significa dar a todo dato el mismo peso, lo que dificulta identificar luego qué es relevante y qué no lo es entre un océano de información irrelevante. [53]

Estamos recolectando tantos datos que nos resulta imposible sacar una imagen clara de todo ello; nuestras mentes no han evolucionado para afrontar tales cantidades de información. Cuando tenemos demasiados datos ante nosotros y tratamos de interpretarlos, nos enfrentamos a dos opciones. La primera consiste en seleccionar información basándonos en algún criterio elegido por nosotros, pero que nos hace perder de vista el contexto, de manera que nuestra comprensión se puede ver reducida, en vez de aumentada. Imagina que riñes con un amigo por culpa del Brexit. Dándole vueltas a vuestra discusión, decides releer todos vuestros mensajes de texto que contengan la palabra «Brexit». Pueden ser mensajes que no ejemplifiquen vuestra relación en su conjunto, sino que solo muestran un desacuerdo puntual. Sin embargo, obsesionarse con ellos puede llevarte a poner fin a vuestra amistad. Si hubieras recordado todos los buenos momentos que habíais pasado juntos y de los que no quedó constancia digital en su día, o si hubieras leído mensajes en los que tu amigo te apoyó cuando estabas pasando por una mala racha, por ejemplo, te habrías acordado de por qué erais amigos.

La segunda opción, cada vez más habitual, para tratar de encontrar un sentido a cantidades desmesuradas de datos consiste en recurrir a algoritmos a modo de filtros que puedan ayudarnos a hilar un relato, aun cuando no tengan incorporado el sentido común necesario para saber qué es importante. Por ejemplo, un algoritmo diseñado para determinar quién es un delincuente analizando imágenes faciales podría acabar seleccionando a aquellas personas que no aparezcan sonriendo. El algoritmo carece de la capacidad racional necesaria para entender que fue entrenado con datos sesgados; las imágenes de delincuentes facilitadas por los cuerpos y fuerzas de seguridad correspondían a fotos tomadas de fichas policiales en las que las personas no sonreían. [54] Además, se ha

demostrado una y otra vez que los algoritmos reflejan sesgos inscritos en nuestros datos, en las suposiciones que hacemos sobre aquello que estamos intentando medir, y en nuestra programación. Hace poco conocí a alguien que decía que se fiaba más de los algoritmos que de los seres humanos porque las personas cometen demasiados errores. Hay que ver con qué facilidad perdemos de vista que son las personas quienes crean los algoritmos y que, muchas veces, la tecnología no solo no corrige nuestros errores, sino que los amplifica.

Así pues, manejar un número excesivo de datos puede llevarnos a saber menos y a tomar peores decisiones. El doble riesgo de tergiversar la verdad y de que los recuerdos sean un obstáculo para el cambio se combina para hacer que los registros extensos y permanentes sobre las personas sean algo muy peligroso. Esos registros recogen los peores momentos de las personas y las congelan en esa imagen, no permitiéndoles superar del todo sus errores. Los viejos datos personales también pueden llevarnos a tener sesgos vinculados con nuestra historia: si usamos información histórica para determinar el futuro, probablemente repitamos los errores del pasado.

Necesitamos introducir fechas de caducidad y olvido en el mundo digital. Podríamos diseñar la tecnología de tal forma que cualesquiera datos generados se autodestruyan después de un tiempo. Algunas aplicaciones ya lo hacen. Por ejemplo, puedes fijar una fecha de caducidad de tus mensajes de texto en Signal. Podríamos hacer algo parecido con los archivos de nuestros ordenadores, con nuestros correos electrónicos, con nuestras búsquedas en línea, con nuestros historiales de compras, con nuestros tuits y con la mayoría de los demás rastros de datos.

Sea cual sea el medio tecnológico que decidamos usar, lo esencial es que la opción marcada por defecto no sea la de conservar nuestros datos personales indefinidamente. Es demasiado peligroso. Necesitamos contar con métodos que permitan la eliminación periódica de datos personales que ya no son necesarios.

Se podría criticar esta idea alegando que no es ético obligar a una sociedad a olvidar. Las democracias no se caracterizan precisamente por forzar el olvido. La quema de libros y el borrado de publicaciones en línea son señales más propias de los gobiernos autoritarios que de los democráticos. La tendencia natural de las sociedades estables que respetan los derechos de los ciudadanos es a acumular datos, vendría a decir ese argumento. Es un razonamiento que resultaría convincente si no tuviéramos la capacidad de retener los datos para siempre. No hay nada de natural en que los registros sean permanentes. La naturaleza nos imponía cierta amnesia a través de nuestra capacidad de olvidar y, ahora que hemos desafiado ese proceso natural, nos estamos empezando a dar cuenta de que el precio a pagar es demasiado alto. Tenemos que volver a introducir ese

elemento natural en un contexto —el del mundo digital— que está del todo alejado de la naturaleza. Para salvaguardar la democracia, lo importante es que los datos nunca se borren por razones ideológicas. Un gobierno, por ejemplo, no debería poder borrar datos que lo dejen en evidencia. Los únicos datos para borrar son los *personales* , y solo en aras de respetar los derechos de los ciudadanos, sin discriminar en función de su contenido político.

Se puede defender, pese a todo, el conservar ciertos tipos de datos personales. Gran parte de lo que hemos aprendido de la historia, por ejemplo, proviene de diarios personales. Hay datos que deberíamos borrar del todo, pero en algunos casos —una minoría— quizá bastaría con encerrar ciertos datos bajo llaves que dificultaran su acceso, o que solo lo permitieran en determinadas circunstancias (por ejemplo, después del fallecimiento de la persona, o cien años después de la fecha de creación de estos). También podemos legar algunos de nuestros datos a nuestros seres queridos y, en particular, a nuestros hijos y nietos, por si les interesara conocer más sobre sus raíces. Si contamos con el consentimiento de las personas pertinentes, tal vez podríamos conservar una pequeña parte de datos personales, protegidos por fuertes salvaguardas, que pudieran ser representativos de una cierta época y lugar, para que los historiadores del futuro puedan aprender de ellos.

Las cerraduras bajo las que se guardarían esos datos no deberían ser únicamente legales (pues las leyes cambian y se incumplen), sino también técnicas (mediante el cifrado, por ejemplo) y prácticas (dificultando el acceso a los datos). En algunos casos, las cerraduras prácticas consisten en trabas físicas. Por ejemplo, si un diario se guarda en papel en una oficina del registro de una localidad, estará accesible a los investigadores serios que quieran estudiarlo, pero será más difícil que accedan a él maleantes que si se publicara en línea y se indexara en los motores de búsqueda. El grado de accesibilidad importa. Ahí radica la esencia del derecho al olvido que se reconoce en Europa.

Cuando Mario Costeja buscó su nombre en Google en 2009, entre los primeros resultados que le aparecieron había un par de anuncios oficiales de finales de la década de 1990 publicados en el diario español *La Vanguardia* . Eran avisos de una subasta pública de compraventa de la casa de Costeja para cubrir las deudas que este entonces tenía con la Seguridad Social. Se habían publicado inicialmente en la versión en papel de dicho periódico y, posteriormente, se digitalizaron.

Costeja acudió a la Agencia Española de Protección de Datos para presentar una queja contra *La Vanguardia* . Alegó que aquellos avisos ya no eran relevantes, puesto que hacía tiempo que había saldado sus deudas. Llevar ese manchón asociado a su nombre estaba perjudicando su vida personal y

profesional. El periódico se había negado a borrar esos registros y la Agencia Española de Protección de Datos falló a su favor, pues consideró que *La Vanguardia* había publicado esos registros públicos de forma lícita. Sin embargo, la agencia dictaminó también que Google debía borrar el enlace a los avisos de subasta que aparecía entre sus resultados. Alguien que ha saldado sus deudas no debería tener que vivir con esa carga durante el resto de su vida.

Google recurrió el dictamen y el caso terminó ante el Tribunal de Justicia de la Unión Europea, que en 2014 falló a favor del derecho al olvido. Los avisos de Costeja todavía se encuentran entre los registros de *La Vanguardia* , pero ya no están indexados en el buscador de Google. Aunque la aplicación práctica de ese derecho ha suscitado dudas y críticas, su principio fundamental tiene sentido. Es cuestionable dejar que sean compañías privadas como Google las que decidan si una petición tiene fundamento, por mucho que esa decisión se pueda recurrir y remitir a una Agencia de Protección de Datos. Sin embargo, lo más importante es que el derecho al olvido nos protege de vernos perseguidos por datos personales «obsoletos, inexactos, inadecuados, irrelevantes o desprovistos de su sentido original, y carentes de todo interés público». [55]

Si no aprendemos de nuevo a olvidar en la era de la máquina, nos quedaremos anclados en el pasado, como sociedades y como individuos. No siempre será fácil, no obstante, asegurarse de que nuestros datos se han borrado o, si no se han borrado, de que podamos supervisar cómo se están usando. Como no disponemos de acceso a las bases de datos de las instituciones, es posible que necesitemos desarrollar formas de rastrear nuestros datos personales.

RASTREAR NUESTROS DATOS PERSONALES

Uno de los mayores desafíos a los que se enfrenta la regulación de los datos personales es la dificultad de controlar dónde están y qué se hace con ellos. En la actualidad, no tenemos más remedio que fiarnos de la palabra de compañías tecnológicas que han demostrado no ser de fiar. Las autoridades de protección de datos en Europa suelen andar cortas de personal y de fondos. Es difícil tener organismos reguladores capaces de supervisar a todas las organizaciones que tratan con datos personales. Los gigantes tecnológicos son más poderosos y ricos que muchos estados. Limitar el uso de los datos personales según las líneas que aquí propongo facilitaría mucho su control, aunque solo fuera por el hecho de tener menos datos personales desparramados por ahí. Sin embargo, siempre serán difíciles de monitorizar.

Que los individuos no tengamos modo alguno de saber quién conserva datos

nuestros nos pone en desventaja. Agrava las asimetrías, ya de por sí preocupantes, entre individuos e instituciones, y hace que la carga de identificar los abusos recaiga casi en exclusiva en los organismos supervisores.

Lo ideal sería que nosotros pudiéramos rastrear nuestros propios datos. Imagina tener una app que pudiera mostrarte un mapa en tiempo real de quiénes tienen tus datos y de cómo los están usando, y que te permitiera retirar al instante esos datos personales tuyos si así lo desearas. Uno de los aspectos más aterradores de la era digital es la posibilidad de que, mientras lees estas palabras, se te esté sometiendo al escrutinio de docenas de algoritmos que estén evaluando tus datos personales y decidiendo tu destino en función de ellos, todo ello sin que lo sepas ni hayas dado tu consentimiento. Justo en este momento, un algoritmo te puede estar etiquetando como insolvente, mientras que otro podría estar decidiendo (basándose, tal vez, en algún criterio erróneo) relegarte varios puestos en la lista de espera para esa intervención quirúrgica que tanto necesitas, y quizá alguno más te esté calificando de inútil para trabajar. Si no sabes cuándo un algoritmo criba tus datos y toma una decisión sobre ti, ¿cómo vas a darte cuenta de que podrías estar siendo víctima de una injusticia? Si no puedes seguir el rastro de quiénes tienen tu información y cómo la están utilizando, ¿cómo puedes tener certeza de que se están respetando tus derechos?

Hay al menos dos grandes retos técnicos asociados a la posibilidad de que las personas rastreen sus datos. El primero es el de hacer corresponder los datos personales con la persona a la que estos se refieren, y garantizar que a todos los individuos se les pida su consentimiento antes de compartir datos sobre ellos. Algunos casos son sencillos: solo se necesita tu consentimiento para que se recolecte o se use tu dirección de correo electrónico. Sin embargo, cuando los datos personales incluyen información sobre más de un individuo, el asunto se complica. Para compartir tus datos genéticos de un modo moralmente aceptable, necesitas el consentimiento de tus padres, hermanos e hijos, como mínimo. Pero ¿y si tus hijos son aún menores y, más adelante, cuando fueran adultos, no quisieran dar su consentimiento? ¿Y tus primos? ¿Hasta qué grado de parentesco tendrías que llegar en tus peticiones de consentimiento? No es fácil responder a estas preguntas porque no podemos estar seguros de qué tipos de inferencias podrán llegar a hacerse sobre tus primos en el futuro con tus datos genéticos. Ante la duda, lo mejor sería optar por la precaución. Quizá no deberíamos permitir que las personas compartan sus datos genéticos, salvo que lo hagan con sus médicos y en el caso de que haya un motivo serio de salud para ello.

El segundo gran reto es idear una forma en la que podamos estar informados de cómo se están usando nuestros datos sin poner aún más en peligro nuestra privacidad. Supone ciertamente un desafío y tal vez no se pueda superar. Es

posible que, al etiquetar los datos personales para poder rastrearlos mejor, nos estemos exponiendo de nuevo y de forma inevitable, lo que malograría el objetivo principal (que no era otro que proteger mejor nuestra privacidad). Está por verse. El creador de la World Wide Web, sir Tim Berners-Lee, trabaja actualmente en un proyecto, Solid, que pretende desarrollar una especie de cápsulas de datos personales que proporcionen a los usuarios un control absoluto sobre su información personal. Si Solid u otro proyecto similar logran vencer estos (y otros) problemas técnicos, podría cambiar drásticamente el modo en que gestionamos nuestros datos personales.

FRENAR LA VIGILANCIA DEL ESTADO

Los gobiernos no necesitan ejercer la vigilancia masiva para proporcionar seguridad a sus ciudadanos. La recopilación y el análisis de datos no deberían tener lugar sin una orden judicial individual (no general) de por medio, y solo cuando sean necesarios. También deberían ser focalizados (a diferencia de lo que ocurre con la vigilancia masiva) y proporcionales a las circunstancias. Según *The New York Times* , en Estados Unidos, un mínimo de dos mil organismos y cuerpos de orden público de los cincuenta estados disponen de herramientas para introducirse sin permiso en teléfonos bloqueados y cifrados, y descargarse sus datos. Y, en ocasiones, esas fuerzas y cuerpos de seguridad practican búsquedas de ese tipo por pequeñas faltas (una investigación por una riña por 70 dólares en un McDonald’s, por ejemplo). Ese no es un uso proporcionado de instrumentos de vigilancia tan invasivos. [56]

Los gobiernos no deberían subvertir la ciberseguridad ni pedir a las empresas que incorporen a sus productos puertas traseras por las que se puedan colar. Para la seguridad nacional es más importante que todos los ciudadanos tengan dispositivos seguros que la facilidad de acceso del Estado a dichos dispositivos, porque, si tu Gobierno puede acceder a ellos, también lo podrán hacer otros agentes, posiblemente perversos.

Las capacidades de vigilancia tienen que estar sometidas a una fuerte supervisión. Estos organismos supervisores tienen que disponer de acceso a toda la información relevante. Debería existir un nivel adecuado de transparencia para garantizar que los ciudadanos conocen las reglas vigentes en su país. A los individuos se les tendría que notificar por adelantado que se les pretende someter a vigilancia antes de que esta sea efectiva o, en el caso de que el aviso anticipado ponga en peligro el avance de la investigación de un delito, debería informárseles de ello *a posteriori* . Las personas a quienes se haya vigilado

tendrían que poder acceder a sus datos, así como disponer de la opción de corregirlos o de añadir información relevante para ponerlos en contexto.

Tenemos que separar el espionaje entre gobiernos de la vigilancia de Estado a los ciudadanos particulares. El espionaje es competencia de las fuerzas armadas y el Ministerio de Exteriores. La vigilancia a ciudadanos privados está justificada solo en el caso de las investigaciones de delitos y es tarea de la policía. Las reglas del espionaje pueden ser secretas. Las de la vigilancia han de ser de conocimiento público. Tanto el espionaje como la vigilancia deberían focalizarse en blancos específicos. [57]

Los denunciantes (*whistleblowers*) tendrían que contar con la debida protección legal frente a posibles represalias. Esos denunciantes son los canarios morales de esta mina que es nuestra sociedad. Los canarios son más sensibles que los seres humanos a gases tóxicos como el monóxido de carbono y por eso los mineros los usaban para detectar situaciones de peligro. En cierto sentido, quienes denuncian prácticas abusivas son más sensibles a la injusticia que la mayoría. Nos alertan de situaciones de peligro para la sociedad. Cuando el canario mostraba síntomas de intoxicación por monóxido de carbono, los mineros lo reanimaban con un tanque de oxígeno. Tenemos que asegurarnos de tener tanques de oxígeno para nuestros denunciantes.

Los metadatos son datos acerca de los datos. Son información que los ordenadores precisan para funcionar y constituyen un subproducto de dicho funcionamiento. La mayoría no se pueden cifrar, porque, si se cifraran, los ordenadores no podrían comunicarse entre sí. Eso hace que sean problemáticos para la privacidad. Para limitar la vigilancia de los metadatos, tal vez sería buena idea dispersar el tráfico de internet para que no se concentre en exceso en unos pocos centros de datos, y deberíamos recurrir más al llamado «enrutamiento cebolla» (una técnica dirigida a preservar el anonimato).

En los metadatos se incluye información como el sistema operativo con el que se crearon los datos, la hora y el día de su creación, el autor de estos y la ubicación en la que se crearon. Los metadatos son un contenido más sensible de lo que parece. De ellos se pueden inferir cosas como, por ejemplo, si alguien planea tener un aborto. «Si cuentas con metadatos suficientes, en realidad no te hace falta el contenido», dijo en una ocasión el antiguo director de servicios jurídicos de la Agencia de Seguridad Nacional (NSA) Stewart Baker. «Matamos a personas basándonos en metadatos», dijo por su parte el general Michael Hayden, exdirector de la NSA y de la CIA. [58] Deberíamos esforzarnos al máximo por impedir que los regímenes autoritarios tengan acceso a los metadatos a través de la infraestructura de internet.

PROHIBIR HERRAMIENTAS DE VIGILANCIA

Algunas tecnologías de vigilancia son tan peligrosas, tan propensas a que se abuse de ellas, que quizá sería mejor prohibirlas por completo, tal y como prohibimos ciertas armas por ser demasiado crueles y peligrosas. Deberíamos prohibir el reconocimiento facial, del andar o de la frecuencia cardiaca de los individuos, entre otras tecnologías que destruyen el anonimato, por constituir herramientas idóneas para la opresión. [59] En una democracia, es necesario que los ciudadanos podamos protestar en las calles anónimamente. También son idóneos para la opresión los receptores IMSI, los programas diseñados para introducirse sin permiso en los teléfonos inteligentes, y otros tipos de software espía; deberían ser ilegales. [60] Según los términos de una demanda judicial reciente, un programa informático diseñado por la compañía israelí NSO Group, especializada en vigilancia, se ha usado para jaquear los teléfonos de activistas, abogados, periodistas y docentes e investigadores universitarios. [61] Además de las tecnologías de identificación y de los programas espía, los satélites y drones de alta resolución representan un tercer tipo de vigilancia que también deberíamos evitar. [62]

Hace unos años, se promovió un proyecto de satélites centinela para captar imágenes que se pudieran usar en un sistema de alerta temprana que impidiera que se pudieran perpetrar atrocidades masivas en Sudán. Dos días después de que el proyecto publicara imágenes satelitales de una nueva carretera sudanesa que se creía podría utilizarse para el transporte de armas, un grupo rebelde lanzó una emboscada contra un conjunto de trabajadores de la construcción en las proximidades de uno de los cruces visibles en una de las fotos y secuestró a veintinueve personas. El momento de la publicación de las imágenes y el del ataque sugieren que podrían estar relacionados. [63] Publicar imágenes satelitales de alta resolución puede ser peligroso. Will Marshall y su equipo de Planet Labs ya toman imágenes de todo el planeta a diario a través de satélites. Ahora se han propuesto indexar todos los objetos del mundo para que puedan aparecer en las búsquedas de información. *Cualquiera* podría vigilarte usando sus satélites. Que se les permita realizar ese trabajo y que lo presenten sin hacer mención alguna a la privacidad es muy alarmante. [64] El cielo no debería estar observándonos.

Hay en marcha una carrera por cartografiar el mundo público y privado, por crear un duplicado digital de nuestro mundo físico. ¿Te imaginas lo poderoso que podría llegar a ser un régimen autoritario si dispusiera de un mapa detallado en tiempo real de todas las habitaciones y edificios del mundo (incluyendo los muebles y las personas que viven en esos espacios)? Si tienes el último robot

aspirador Roomba, es probable que ya haya creado un plano de tu domicilio. [65] Amazon ha anunciado hace poco el futuro lanzamiento al mercado de un dron autónomo para interiores que puede mapear tu hogar y vigilar mejor a tu familia. [66] Según el vídeo promocional del Proyecto Aria de Facebook, esta plataforma ya está dejando que «unos cientos de trabajadores» vayan con sus gafas inteligentes puestas «por diversos campus y espacios públicos». En el vídeo se mencionan ciertas ventajas de tener el mundo cartografiado, como, por ejemplo, poder encontrar tus llaves fácilmente. [67] No merece la pena renunciar a nuestra privacidad. Hay otras formas de encontrar tus llaves sin necesidad de crear una copia virtual en tiempo real de la realidad. ¿Qué derecho tiene Facebook —una compañía privada con uno de los peores historiales en materia de privacidad— de crear un duplicado de nuestro mundo para que nos pueda vigilar mejor? Ninguno. Esa clase de datos no deberían pertenecer a ninguna corporación. Hay aspectos y rincones de la realidad que nunca deberían convertirse en datos.

Financiar la privacidad

Además de invertir en el desarrollo de herramientas de privacidad, necesitamos una mejor gobernanza de los datos. Hay que financiar mejor y dotar de más personal a los organismos reguladores que están a cargo de la protección de los datos. Para que estas autoridades tengan la más mínima posibilidad de hacer frente a los titanes tecnológicos, tenemos que proporcionarles herramientas suficientes. Algunas de las sugerencias aquí mencionadas ya forman parte de leyes como el Reglamento General de Protección de Datos (RGPD) y la Ley de Privacidad del Consumidor de California. Sin embargo, hasta ahora, las agencias de protección de datos de los países europeos se han visto abrumadas por la tarea que se les ha encomendado y para la que no disponen de suficientes recursos. [68] Primero tenemos que prestar todo nuestro apoyo a los organismos protectores de la privacidad a fin de garantizar el cumplimiento de la ley. Y luego debemos imponer las regulaciones necesarias para acabar con la economía de los datos de una vez por todas.

Crear organismos reguladores de lo digital

La Unión Europea, Australia y Reino Unido ya están valorando la creación de un regulador de las grandes compañías tecnológicas. Tiene sentido hacer lo mismo en Estados Unidos. Si en ese país existe una Comisión de Valores y Bolsas para

los mercados financieros, una Administración Federal de Aviación para las aerolíneas, una Administración de Alimentos y Medicamentos para las farmacéuticas, y una Comisión Federal de las Comunicaciones para las telecos, las grandes tecnológicas bien merecerían su propia agencia supervisora especializada. [69]

Actualizar las leyes antimonopolio

La regulación antimonopolio tiene que responder al verdadero carácter del poder en la era digital. Si una empresa puede fijar unos términos de servicio abusivos sin perder usuarios, debería abrírsele una investigación, independientemente de si les cobra a sus usuarios.

Es posible que las grandes compañías tecnológicas sean ya tan poderosas que necesitemos dividirlas antes para poder regular de forma adecuada el ámbito de los datos personales. Los pesimistas tienden a pensar que las grandes tecnológicas han alcanzado tal volumen que hemos perdido la oportunidad de seccionarlas o de regularlas, pero esta valoración carece de perspectiva histórica. Hemos regulado todas las demás industrias precedentes. ¿Por qué iban a ser distintas las tecnológicas? La demanda judicial por parte del Departamento de Justicia de Estados Unidos contra Google este mismo año podría señalar el inicio de un enfrentamiento serio con las grandes tecnológicas. No obstante, una preocupación justificada es que las demandas antimonopolio pueden ser muy lentas (la causa contra Microsoft, por ejemplo, duró ocho años) y las grandes tecnológicas continúan creciendo rápidamente. Por eso debemos recurrir a múltiples enfoques para regular estos gigantes empresariales y no apostarlo todo a uno en exclusiva. Un motivo de optimismo es que hay muchos países que quieren regular las tecnológicas. Si colaboran y se coordinan unos con otros, la existencia de un objetivo común puede dotar a sus respectivas competencias reguladoras de una mayor fuerza y capacidad de influencia.

Desarrollar la diplomacia de los datos

Como en el caso del cambio climático, la privacidad representa un problema de acción colectiva y los acuerdos internacionales serán instrumentos importantes para la protección de los datos personales. Los flujos de datos rara vez respetan las fronteras. [70]

Si los países actúan de un modo excesivamente individualista, podríamos presenciar la aparición de «paraísos de datos», análogos a los fiscales. Serían

países cómplices con el «lavado de datos» por su disposición a alojar información obtenida por vías ilícitas que luego se reciclaría en forma de productos aparentemente respetables. Esos datos también se podrían usar para entrenar a programas informáticos espía que se venderían a cualquiera que estuviera dispuesto a pagar por ellos, regímenes autoritarios incluidos. [71] La presión internacional tendrá una importancia capital para mejorar los estándares de privacidad en todas partes.

Otro ámbito en el que necesitamos trabajar diplomáticamente es el relacionado con el tipo de datos que las agencias de inteligencia aliadas estarían autorizadas a compartir. Podemos llegar a implantar buenas normativas para frenar la vigilancia de Estado dentro de las fronteras de nuestro país, pero todo ese esfuerzo sería en vano si nuestro Gobierno puede adquirir los datos personales de sus ciudadanos tomándolos de otro país (por ejemplo, Estados Unidos y Reino Unido suelen compartir datos). En muchas ocasiones, las democracias desconocen qué datos tienen sus propios gobiernos de ellas porque estos se escudan en que carecen de autoridad para revelar datos recopilados originalmente por una agencia de inteligencia de un país aliado. Necesitamos normas claras y una mayor transparencia sobre qué datos son los que nuestras agencias de inteligencia pueden solicitar a otros países.

PROTEGER A NUESTROS NIÑOS

Debemos proteger a todas las personas, pero a los niños en particular, porque estos se encuentran en una situación de excepcional vulnerabilidad. Los niños pequeños dependen de sus familias y de sus escuelas para proteger su privacidad. Y la tendencia actual es a vigilarlos desde el momento en que son concebidos, con la excusa de mantenerlos a salvo.

Hay dos razones fundamentales para preocuparse por la privacidad de los niños en especial. En primer lugar, la vigilancia puede poner en riesgo su futuro. No queremos que las oportunidades de nuestros hijos queden comprometidas porque las instituciones los juzguen (a partir de errores algorítmicos, posiblemente) en función de determinados datos recopilados sobre su salud, sus capacidades intelectuales o su comportamiento en el colegio o con sus amigos. En segundo lugar, y más importante aún, el exceso de vigilancia puede quebrantar el carácter de las personas. Educar a los niños bajo un régimen de vigilancia continua significa criar súbditos, no ciudadanos. Y queremos ciudadanos. Por su propio bien y por el bien de la sociedad.

La sociedad necesita ciudadanos autónomos y comprometidos, capaces de

cuestionar y transformar el *statu quo* . Los grandes países no están constituidos por seguidores serviles. Para convertirse en personas con corazones y mentes fuertes, los niños necesitan explorar el mundo, equivocarse y aprender de sus experiencias sabiendo que no quedará constancia de sus errores, y que estos no se usarán en su contra en el futuro. La privacidad es necesaria para cultivar la audacia.

Debido probablemente a su extrema vulnerabilidad, los niños y, en particular, los adolescentes tienden a ser más sensibles que los adultos a lo que otros piensan de ellos. Por ello la vigilancia puede resultarles aún más opresiva. Los jóvenes que estén siendo observados en todo momento serán menos propensos a intentar algo nuevo, algo que se les pueda dar mal al principio, pero que bien podrían dominar con la práctica y el tiempo si se les dejara en paz para fallar y hacer el ridículo sin público presente.

Lo que hace más difícil el caso de los niños es que es verdad que precisan de cierta supervisión para que estén seguros. El riesgo es que la seguridad se utilice como pretexto para someterlos a una vigilancia indebida. La línea que separa lo necesario de lo injustificado en ese terreno no siempre es clara.

Los defensores de la vigilancia en las escuelas sostienen que así se «educa» a los alumnos en cómo ser buenos «ciudadanos digitales», y se les acostumbra a la vigilancia omnipresente de la que serán objeto cuando terminen sus estudios. «Escoja a cualquier persona adulta que tenga un empleo y verá que esta no puede escribir lo que le dé la gana sin más en el correo electrónico de su trabajo; la están observando —decía no hace mucho Bill McCullough, un portavoz de Gaggle, empresa estadounidense dedicada a la monitorización de centros educativos—. Nosotros preparamos a los chavales para que sean adultos exitosos.» [72] No. Lo que hace el exceso de vigilancia es enseñar a los niños que los derechos humanos son algo que no se tiene que respetar. No es realista suponer que personas a las que, de niños, se les ha enseñado que sus derechos no importan vayan a mostrar respeto alguno por los derechos de los demás cuando sean adultos.

Vigilar a los niños desde el principio para que se acostumbren a ello cuando lleguen a su vida adulta es como implementar un sistema de calificaciones totalmente injusto en el colegio para que los niños se acostumbren a lo injusta que es la vida. Si no aceptamos esto, tampoco deberíamos aceptar lo primero. Un sistema de calificaciones justo no solo da a todos los niños un acceso equitativo a las oportunidades, sino que a su vez les enseña a esperar un trato justo de parte de las instituciones, algo que, más adelante en la vida, también los animará a exigir justicia, así como a luchar por ella y crearla cuando no se les ofrezca. Lo mismo ocurre con la privacidad.

La vigilancia lleva a la autocensura. Es una advertencia para que los alumnos no traspasen límites, para que no hablen de temas delicados y ni siquiera los busquen en internet; cualquier comportamiento fuera de los límites de lo que es política y socialmente seguro podría desencadenar una investigación escolar o incluso policial. Sin embargo, la adolescencia es sinónimo de sentir curiosidad por las cosas de la vida. Los jóvenes se hacen preguntas sobre el sexo, las drogas y la muerte, entre otros temas delicados, y desalentar su exploración personal en esos terrenos no contribuye a su conocimiento ni a su madurez. En cierto sentido, cuando supervisamos demasiado a los jóvenes, coartamos el proceso por el que se van convirtiendo en adultos responsables que no necesitarán supervisión. Cuando vigilamos en exceso a los niños, cuando los oprimimos bajo el control de una especie de policía del pensamiento, corremos el riesgo de estar criando a una generación de personas a las que nunca se les permitió crecer.

Hay mucho que puedes hacer para proteger la privacidad de tus hijos. Sin embargo, antes de que pasemos a analizar lo que está en nuestras manos, como individuos, para proteger la privacidad, hay una objeción habitual a todo lo anterior a la que merece la pena responder.

¿NO NECESITAMOS LOS DATOS PERSONALES?

Los entusiastas de la economía de los datos seguramente te dirán que desenchufar el cable de alimentación del actual torrente de datos personales obstaculizaría la innovación. La versión más alarmista de esta tesis viene a decir que, si regulamos la economía de los datos, otras potencias extranjeras (y posiblemente rivales) desarrollarán la inteligencia artificial (IA) más rápido que nosotros y nos quedaremos rezagados. Limitar lo que podemos hacer con los datos es poner freno al progreso, versa este argumento.

La respuesta corta a esta objeción es que «no»: *progreso* es defender los derechos humanos de las personas y no socavarlos. Los defensores de las tecnologías han tendido a exagerar de forma sistemática las ventajas de la economía de los datos en términos de rentabilidad económica, avance científico y seguridad, al tiempo que han restado importancia a sus costes.

Hay también una respuesta más larga. Incluso si entendiéramos «progreso» solamente como progreso tecnológico, la respuesta seguiría siendo que «no»: la protección de la privacidad no tiene por qué ser a expensas del avance de la tecnología. No olvidemos que los datos personales se utilizan en gran parte para sacarles un provecho económico. Es posible que empresas como Google no se vean obligadas siquiera a innovar para tener un modelo de negocio sostenible.

Quizá, en sus comienzos, las posibilidades que Google tenía de vender directamente sus servicios a los consumidores no eran muchas. Los consumidores aún no habían saboreado lo suficiente los beneficios de navegar por su vida cotidiana con la ayuda del buscador, los mapas y otros productos de Google. En la actualidad, sin embargo, los ciudadanos de la red sí se han hecho ya una buena idea del valor de dichos productos. Pues bien, paguemos por ellos si tanto los valoramos. En 2013, a Google le iba ya extraordinariamente bien. Contaba con unos 1.300 millones de usuarios y registraba unos ingresos anuales de unos 13.000 millones de dólares. Ganaba al año unos 10 dólares de media con cada usuario. [73] ¿No sería ese un precio razonable por recibir los servicios de Google? Es menos de lo que se paga por servicios de entretenimiento como Netflix, que cuestan algo más de 10 dólares mensuales.

Al permitir que los datos personales sean rentables, incentivamos que se recopilen más de los necesarios para el progreso tecnológico. La idea es que el uso de datos con fines científicos y tecnológicos siga estando permitido, pero que, si las instituciones y organizaciones quieren experimentar con datos *personales* , tengan que asumir las responsabilidades correspondientes para respetar los derechos de las personas. Es una exigencia razonable. Si las compañías tecnológicas logran transformar sus iniciativas en servicios valiosos para los ciudadanos de la red, estaremos encantados de pagar por ellos, igual que lo hacemos por otras cosas que apreciamos en el mundo analógico.

Además, no está ni mucho menos claro que contar con existencias infinitas de datos personales favorezca necesariamente el progreso tecnológico y científico. Como ya hemos visto, el exceso de datos puede dificultar el pensamiento y la toma de decisiones. Inyectar más datos en un mal algoritmo no lo convertirá en bueno. Cuando diseñamos inteligencia artificial (IA) aspiramos a fabricar precisamente eso, inteligencia. Si has interactuado últimamente con algún asistente digital, te habrás dado cuenta de que no son muy listos.

Los seres humanos pueden aprender cosas nuevas con un ejemplo y transferir ese conocimiento a otras situaciones similares. A medida que los sistemas de IA se vayan haciendo más inteligentes, cabrá esperar de ellos que necesiten menos datos. [74] Los desafíos más importantes a los que se enfrenta el desarrollo de la IA son técnicos y no se van a resolver arrojando más datos al problema. [75] No es de extrañar que las aportaciones posiblemente más sofisticadas de la IA hasta la fecha no hayan surgido del aprovechamiento de los datos personales.

AlphaZero es un algoritmo desarrollado por DeepMind (una empresa del conglomerado de Google) que juega al antiguo juego chino del go (así como al ajedrez y al *shogi*). Lo que hace que el go sea un juego de especial interés para la IA es, para empezar, su complejidad. Comparado con el ajedrez, el go se juega

en un tablero más grande y son muchas más las alternativas que hay que considerar en cada jugada. El número de movimientos posibles desde una posición dada es de, aproximadamente, veinte en el ajedrez; en el go son unos doscientos. El número de configuraciones posibles del tablero supera el número de átomos en el universo. En segundo lugar, el go es un juego en el que se cree que la intuición juega un gran papel. Cuando preguntan a los jugadores profesionales por qué han hecho un movimiento en particular, muchas veces responden con algo así como que «tenían una corazonada». Es ese carácter intuitivo el que hace que muchas personas consideren el go un arte y a los jugadores de go, unos artistas. Por lo tanto, para que un programa informático pueda vencer a jugadores humanos de go tiene que imitar la intuición humana o, más precisamente, igualar los resultados de esta.

Lo más extraordinario de AlphaZero es que fue entrenado *exclusivamente* a base de jugar contra sí mismo. No utilizó datos externos. AlphaGo, el algoritmo que precedió a AlphaZero, sí se entrenó en parte con cientos de miles de partidas de go jugadas anteriormente entre jugadores humanos. DeepMind tardó meses en entrenar a AlphaGo para que fuera capaz de derrotar al campeón del mundo, Lee Sedol. AlphaZero desarrolló aptitudes sobrehumanas para el juego del go en solo tres días. Y sin datos personales.

¿Y LA MEDICINA?

La medicina constituye un caso muy especial en el mundo de los datos. Primero, porque la medicina es muy importante para todos nosotros. Todos queremos vidas más largas y sanas. Todos queremos que la medicina progrese lo más rápido posible. Segundo, porque los datos médicos son muy delicados, ya que pueden conducir a la estigmatización, la discriminación o cosas peores. Tercero, porque anonimizar datos médicos es extremadamente difícil y en ocasiones imposible. Los datos genéticos, como ya hemos visto, son un buen ejemplo: son datos que te identifican de forma exclusiva y específica, que incorporan tu propia identidad. En general, para que los datos médicos resulten útiles, es importante identificar qué datos pertenecen a una misma persona y, cuantos más datos tengamos sobre alguien, más fácil será identificarlo.

Ahora bien, ¿depende el avance de la medicina del *comercio* de los datos personales? No. En primer lugar, deberíamos ser un poco más escépticos sobre las capacidades de la tecnología digital. En segundo lugar, hay formas de usar los datos personales para la investigación médica que minimizan el riesgo para los pacientes y piden su consentimiento previo. Y, en tercer lugar, es posible que

algunos de los avances médicos más importantes no precisen del uso de datos personales. Examinemos algo más detenidamente estos tres argumentos.

La tecnología digital médica en perspectiva

La tecnología digital y los macrodatos no son mágicos. No podemos esperar que resuelvan todos nuestros problemas. A veces, las innovaciones que salvan más vidas no son las de la alta tecnología, sino cambios menos glamurosos, como mejores prácticas de higiene. Esto no quiere decir que la alta tecnología no pueda aportar nada a la medicina, pero no deberíamos renunciar a nuestro razonamiento crítico cuando hablamos de las tecnologías digitales. Cuando lo tecnológico se convierte en ideológico, como en ocasiones ocurre, se aparta de la ciencia y se aproxima a la superstición. He aquí dos ejemplos de cómo la tecnología digital ha prometido más de lo que ha conseguido en el contexto de la medicina.

El primer caso es el sistema de inteligencia artificial de IBM, Watson. En 2011, después de que Watson derrotara a dos campeones humanos del concurso televisivo estadounidense de preguntas y respuestas *Jeopardy* !, IBM anunció que su sistema de IA estaba preparándose para hacer las veces de un médico. Según la compañía, los primeros productos comerciales con el sello Watson estarían listos en un plazo de dieciocho a veinticuatro meses. Nueve años después, esa promesa aún no se ha cumplido.

En 2014, IBM invirtió 1.000 millones de dólares en Watson. En 2016, había adquirido cuatro empresas especializadas en datos de salud por una suma total de 4.000 millones de dólares. Sin embargo, muchos de los hospitales que se han involucrado con proyectos con IBM Watson han tenido que ponerles fin. El hospital MD Anderson Cancer Center tuvo que cancelar su colaboración con Watson para el desarrollo de una herramienta de asesoramiento para oncólogos tras haberse gastado 62 millones de dólares en ella. [76] En Alemania, el hospital universitario de Giessen y Marburgo también tiró la toalla. Cuando un médico le indicó a Watson que tenía un paciente con dolor en el pecho, el sistema no consideró la posibilidad (más probable) de que estuviera sufriendo un ataque cardiaco, sino que sugirió como diagnóstico una enfermedad infecciosa rara. [77] En otra ocasión, Watson recomendó que se administrase a un paciente de cáncer que sufría una hemorragia grave un fármaco que podría haberla empeorado. «Este producto es una m...», sentenció un médico del Jupiter Hospital de Florida. [78]

Watson no ha sido el único caso en el cual la tecnología digital nos acaba

decepcionando en el campo de la medicina. En 2016, DeepMind cerró un acuerdo con la fundación hospitalaria pública Royal Free de Londres que le dio acceso a los historiales médicos de 1,6 millones de pacientes sin el consentimiento ni el conocimiento de estos. Eso significa que la empresa pudo consultar informes patológicos, exámenes radiológicos, estados de VIH, detalles sobre episodios de sobredosis de drogas, quién había tenido un aborto, quién tenía cáncer, y más. [79] La Oficina del Comisionado de Información (ICO) dictaminaría más tarde que Royal Free había infringido las leyes de protección de datos. [80]

La idea original de ese acuerdo consistía en usar la IA de DeepMind para desarrollar una aplicación que detectara lesiones renales agudas. Los investigadores enseguida se dieron cuenta de que no disponían de datos lo suficientemente buenos para usar la IA y tuvieron que conformarse con algo más sencillo. Al final, Streams, la app resultante de todo ese proceso, no ha tenido «ningún efecto beneficioso estadísticamente significativo en los resultados clínicos de los pacientes». [81]

Estos dos fracasos no implican que a todos los intentos les vaya a suceder lo mismo, pero sí nos brindan una mejor perspectiva desde la que valorar las promesas de la tecnología digital en medicina. En un metaanálisis reciente, se examinaron unos 20.000 estudios sobre sistemas médicos de IA que presumían ser capaces de diagnosticar enfermedades igual de bien que los médicos. Los investigadores hallaron que solo 14 de esos estudios (menos del 0,1 por ciento del total) tenían una calidad metodológica suficiente como para testar esos algoritmos en un entorno clínico real. [82]

Que la IA médica pueda no ser de mucha ayuda para los pacientes no es la única preocupación que suscita esa tecnología. Más inquietante resulta la posibilidad de que termine perjudicándolos. Por ejemplo, la IA podría inducir al sobretratamiento. Algunas tecnologías digitales médicas parecen caer en un exceso de falsos positivos (detectando problemas médicos cuando no los hay). Ciertos algoritmos que buscan células cancerosas, por ejemplo, etiquetan como anómalas células perfectamente sanas a una media de ocho falsos positivos por imagen. [83] Si empresas y médicos tienen algún incentivo (económico, profesional o motivado por los datos) para intervenir en los pacientes, esta tendencia a sobrediagnosticar podría conducir a un problema de sobretratamiento.

Otro posible problema son los fallos técnicos. Es peligroso depender de la tecnología digital porque programar es una labor extremadamente difícil, y la tecnología digital tiene muchas más necesidades que la tecnología analógica. Todo ello hace que la tecnología digital sea muchas veces menos robusta.

Compara un libro electrónico con uno en papel. El dispositivo de lectura de libros electrónicos necesita recargarse cada cierto tiempo, se puede jaquear, depende de una conexión a internet, se puede estropear si se cae en la arena, en el agua o sobre una superficie dura, etcétera. En cambio, los libros de papel son extraordinariamente resistentes. No tienen una batería que haya que recargar y, si los dejas caer desde lo alto de un edificio, probablemente sobrevivan (aunque el transeúnte sobre el que caiga puede que no, así que mejor que no lo intentes). Cuando se trata de equipos médicos que pueden salvar vidas, queremos una tecnología tan robusta como la de los libros de papel.

Estos fracasos aportan algo de realismo y de perspectiva al potencial de la tecnología digital en medicina. Por supuesto, la IA podría terminar desempeñando un papel muy importante en el progreso médico. Sin embargo, como con cualquiera otra intervención, necesitamos que se fundamente en pruebas sólidas antes de entregarle nuestros datos personales, y también necesitamos ciertas garantías de que nuestros datos se manejarán adecuadamente y de que los beneficios serán compartidos de un modo justo y equitativo. Hasta el momento, sin embargo, a la IA se le ha dado carta blanca con demasiada frecuencia.

Supón que decidimos que sí queremos que se realice investigación médica con datos personales y tecnología digital. Después de todo, las promesas de la medicina personalizada son ciertamente atractivas. Hay formas de llevar a cabo investigación que son bastante más éticas que la elegida en su momento por DeepMind y Royal Free.

Investigación médica ética

La ética médica hace mucho tiempo que ayuda a encontrar participantes para ser sujetos de estudios y ensayos. La investigación con datos personales no debería verse como algo muy diferente de otras formas de investigación médica. Aunque la sensación de donar datos personales no tenga nada que ver con la sensación de donar sangre o tejido —no hay aguja ni bisturí ni dolor—, también tiene sus riesgos. Ya no se obliga a nadie a participar en investigaciones clínicas (como sí se hacía en otros tiempos, antes de que se desarrollara la ética médica). Tampoco deberíamos obligar a las personas a participar en investigaciones médicas con sus datos personales. No es aceptable utilizar a los miembros de la población general como conejillos de Indias sin su consentimiento, sin las debidas garantías y sin algún tipo de compensación. Deberíamos pedir el consentimiento de los participantes, fijar algunas normas sobre cómo se usarán sus datos y

cuándo se borrarán, y compensarlos adecuadamente por ello, al igual que hacemos con otros tipos de investigación.

A veces, las instituciones de salud pública no disponen ni de los recursos ni de la tecnología necesaria para analizar datos y podrían beneficiarse de colaborar con empresas privadas. En esos casos, debemos asegurarnos de que los acuerdos que se cierren sean beneficiosos para los sujetos de datos y los pacientes. Entre los muchos errores que cometió Royal Free, dos destacan como particularmente graves. Primero, no se procuró garantía legal alguna de que DeepMind no usaría esos datos para nada más que el desarrollo de la aplicación. Se obtuvo la promesa de que no asociarían esos datos con los que ya tenía Google en su posesión, pero, cuando la división de salud de DeepMind fue absorbida por Google unos años después, expertos en privacidad expresaron su temor a que esa promesa se rompiera. [84]

El segundo gran error fue que Royal Free no se aseguró de que los pacientes se beneficiarían de los productos desarrollados con sus datos. [85] Las instituciones sanitarias públicas poseen tantos datos médicos valiosos que su poder negociador es alto; deberían usarlo. Deberían limitar el acceso de las empresas a esos datos. Tal vez estas podrían usarlos, pero no guardarlos, por ejemplo. Y la sanidad pública debería exigir garantías legales de que cualquier producto desarrollado con esa información se ofrezca luego a las instituciones sanitarias públicas y a la ciudadanía en general a unos precios asequibles.

Siempre habrá que batallar por la seguridad de los datos personales al tratar con compañías que no tienen el bien común como su objetivo principal. Pero, si tenemos suerte, es posible que los avances médicos más importantes que la IA pueda ofrecernos no sean producto de trabajar con datos personales.

Avances médicos sin datos personales

Como hemos visto antes, AlphaZero, ejemplo estrella de la IA, representa un hito extraordinario, pero no tiene aplicaciones prácticas en la vida diaria (todavía). Una manera en la que la IA podría cambiarnos (y salvarnos) la vida es contribuyendo al descubrimiento de nuevos fármacos.

Los antibióticos son, muy probablemente, el avance médico más importante del siglo pasado. Con anterioridad a su descubrimiento, la principal causa de mortalidad en todo el mundo eran las enfermedades infecciosas bacterianas. La mayoría de la gente de los países desarrollados muere hoy mucho más tarde de lo que lo habría hecho si no existieran los antibióticos, a consecuencia sobre todo de dolencias no transmisibles, como las cardiacas o el cáncer. [86] Por desgracia,

la eficacia de estos medicamentos maravillosos está en riesgo por culpa de la resistencia microbiana. A través de procesos evolutivos como las mutaciones, las bacterias se van haciendo resistentes a los antibióticos a los que han estado expuestas. Cuanto más usamos antibióticos, más oportunidades damos a esas bacterias de desarrollar resistencia a ellos. Un mundo sin antibióticos eficaces es una posibilidad tan alarmante como realista. Muchos procedimientos quirúrgicos considerados poco peligrosos pasarían a ser de alto riesgo. Muchas más mujeres morirían por complicaciones en el parto. Una visita al dentista o una aventura de una noche podrían matarte si contraes una infección. La quimioterapia y el trasplante de órganos se convertirían en tratamientos mucho más peligrosos, ya que deprimen el sistema inmune. La resistencia a los antibióticos podría ser un factor que contribuyese de manera importante a una caída en la esperanza de vida.

Necesitamos nuevos antibióticos con urgencia, pero el proceso de descubrimiento y desarrollo de nuevos fármacos es lento y caro. No obstante, unos investigadores del MIT creen que podrían haber dado con una nueva manera de crear nuevos medicamentos antibióticos. Después de suministrar información a un ordenador sobre las características atómicas y moleculares de miles de fármacos y de compuestos naturales, entrenaron a un algoritmo para que identificara tipos de moléculas capaces de matar bacterias. Luego proporcionaron al algoritmo una base de datos de 6.000 compuestos. Este seleccionó una molécula sobre la que infirió un fuerte poder antibacteriano y que —y esto es importante— posee una estructura química diferente de la de los antibióticos existentes.

Este modelo informático puede examinar más de 100 millones de compuestos químicos en unos pocos días, algo que resultaría imposible en un laboratorio normal. [87] Se espera que este nuevo antibiótico, la halicina, sea potente y actúe por vías nuevas a las que las bacterias todavía no han desarrollado resistencia. Podrían producirse avances similares en el descubrimiento de medicamentos antivirales y antifúngicos, así como de vacunas. Si la IA nos ayuda a vencer en nuestra carrera armamentística contra los supermicrobios, se habrá ganado su lugar en la medicina.

El que dos de los avances más destacados en IA se hayan producido sin uso de ningún tipo de datos personales puede no ser casualidad; los datos personales a menudo son imprecisos y pueden quedarse desfasados o caducar con relativa rapidez (por ejemplo, si te cambias de casa).

La conclusión es que, si protegemos nuestra privacidad, no estaremos obstaculizando el desarrollo de la IA. Podemos usar datos personales, con las debidas precauciones, pero no tenemos por qué convertirlos en una mercancía. Y

tal vez no los necesitemos para la mayoría de los avances. El verdadero progreso se define por la protección de los derechos de los ciudadanos y la mejora del bienestar de las personas. El comercio de datos personales no contribuye a esos objetivos.

CUIDADO CON LAS CRISIS

En el momento de escribir este capítulo, la pandemia de coronavirus sigue causando estragos. Diversas compañías de tecnología y telecomunicaciones de todo el mundo han ofrecido a los gobiernos sus servicios de recopilación y análisis de datos para intentar frenar el contagio. Google y Apple acordaron unir fuerzas para modificar su software con el fin de contribuir al desarrollo de aplicaciones de rastreo de contactos. [88] Corren tiempos peligrosos para la privacidad. Cuando el ambiente que se respira es de pánico, tendemos a estar más dispuestos a renunciar a derechos civiles a cambio de una mayor sensación de seguridad. Pero ¿harán esas apps del coronavirus que estemos más seguros? No está nada claro.

La Universidad de Padua llevó a cabo un estudio en la localidad de Vò, donde se registró el primer fallecimiento por coronavirus en Italia. Los investigadores realizaron pruebas a todos los habitantes. Descubrieron que las personas infectadas pero asintomáticas jugaban un papel fundamental en la propagación de la enfermedad. Detectaron 66 casos positivos a los que aislaron durante catorce días. Tras esas dos semanas, 6 casos seguían dando positivo en el test del virus. Tuvieron que continuar en aislamiento. A partir de ahí, ya no hubo nuevos casos. La infección había quedado completamente bajo control. No se necesitó ninguna app. [89]

Las aplicaciones de rastreo de contactos siempre serán menos precisas que las pruebas; les dirán a algunas personas que se queden en casa, aunque no se hayan contagiado (por mucho que hayan estado cerca de alguien que esté infectado), y dejarán que otras que sí están infectadas (y sí deberían aislarse) se muevan con libertad. Las apps no pueden sustituir a las pruebas porque funcionan a partir de indicios representativos (*proxies*) o inferencias.

Lo que necesitamos saber es si alguien ha contraído el coronavirus. Lo que hacen las aplicaciones es tratar de encontrar formas de inferir una infección. Todas ellas, sin embargo, presentan problemas, porque lo que una app entiende como «contacto» no es lo mismo que infectarse. Las aplicaciones suelen definir un «contacto» como el haber estado cerca (a menos de dos metros) de otra persona durante quince minutos o más. Lo primero que hay que advertir es que

las aplicaciones funcionan en teléfonos. Si no llevas tu teléfono contigo, la app no sirve. Supón que todos lleváramos nuestros teléfonos encima (tal vez porque se impusiera por obligación legal, lo cual no dejaría de ser gravosamente invasivo); podríamos rastrear contactos por GPS o por *bluetooth* , pero ninguna de las dos vías es perfecta.

La aplicación podría identificar a dos personas como si estuvieran «en contacto» cuando, en realidad, se hallan en plantas diferentes de un mismo edificio, o en la misma planta, pero separadas por una pared. Si esos dos usuarios reciben el aviso de que podrían haberse contagiado, constituirán dos casos de falsos positivos. Pero también cabe esperar que esas aplicaciones produzcan un elevado número de falsos negativos. Supón que te encuentras con una amiga en la calle y que hace tanto que no os veíais que os dejáis llevar por el impulso y os dais un abrazo y un beso sin pensarlo. Es posible que te hayas infectado con ese gesto y que la aplicación no sospeche de ti porque entienda que no pasaste quince minutos o más con esa otra persona. O puede que te hayas contagiado por contacto con una superficie contaminada. En cualquiera de esos casos, la app no te identificaría como alguien que esté corriendo un riesgo; de hecho, podría estar contribuyendo a generar una falsa sensación de seguridad que haga que las personas actúen con menos cuidado del que de otro modo tendrían.

Rastrear a todo el mundo mediante aplicaciones cuando, en muchos países, solo se está realizando la prueba de detección del virus a personas hospitalizadas o con síntomas no tiene mucho sentido. Las apps notificarán a personas que hayan estado en contacto con otras que hayan dado positivo en una prueba de coronavirus, sí, pero para entonces los individuos notificados ya habrán contagiado a otros que, a su vez, habrán infectado a unos cuantos más. Y como muchos de ellos habrán seguido siendo asintomáticos, habrán continuado también propagando la infección.

La mayoría de las personas contagiadas no necesitarán ir al hospital y no se harán una prueba. Para contener la propagación del virus, necesitamos, por lo tanto, o bien pruebas en masa, o bien vacunas, o ambas cosas. Y, si se realizaran pruebas en masa, no está claro en qué sentido nos beneficiarían las aplicaciones. Si tuviéramos acceso a unas pruebas de detección del coronavirus baratas y fáciles de realizar, hasta el punto de que cada persona pudiera hacerse un test diario en casa, no necesitaríamos ninguna app, pues ya sabríamos quién tiene el virus, quién tiene que quedarse en casa y quién puede salir a la calle. Casi un año después haber empezado la pandemia, la mayoría de los países continuaban sin tener la capacidad de hacer pruebas en masa.

Circula por ahí un peligroso relato sobre la situación actual que viene a decir

que lo que permitió que China controlara mejor la pandemia que países democráticos fue su autoritarismo y, en particular, el uso que sus autoridades hicieron de una aplicación muy invasiva. En realidad, lo más probable es que su sistema de pruebas en masa fuera lo que más contribuyó al control de la enfermedad. En mayo de 2020, China realizó pruebas a toda la ciudad de Wuhan en diez días. En octubre de 2020, hizo lo mismo con los nueve millones de habitantes de la ciudad de Qingdao después de que se hubieran detectado allí doce casos de infección. [90] Ningún país occidental ha llevado a cabo pruebas en masa a semejante escala.

Además de su imprecisión, cualquier aplicación introduce también riesgos para la privacidad y la seguridad. La forma más fácil de jaquear un teléfono es a través de su *bluetooth* . Si usáramos la app, cualquier persona entendida en tecnología podría potencialmente enterarse de quién la infectó a ella o a algún ser querido, una información bastante peligrosa cuando hablamos de una enfermedad que puede ser mortal. O alguien podría utilizar el sistema para, por ejemplo, vigilar a los usuarios de la aplicación, o para generar mapas de calor de dónde se encuentran las personas contagiadas. Yves-Alexandre de Montjoye y su equipo han calculado que, con los rastreadores instalados en los teléfonos de un 1 por ciento de la población londinense, un atacante podría conocer la ubicación en tiempo real de más de la mitad de los habitantes de la ciudad. [91] Hay que recordar que la privacidad es colectiva.

Entonces ¿por qué hubo un momento al principio de la pandemia en el que se dio prioridad a las aplicaciones y no a hacer pruebas exhaustivas a la población? Tal vez porque son más baratas. Tal vez porque las compañías tecnológicas son las grandes corporaciones empresariales por excelencia en la actualidad y, siempre que hay una crisis, se les pide ayuda a las grandes empresas. Si las mayores compañías mundiales fuesen del sector industrial, tal vez la ayuda ofrecida habría sido en forma de producción de desinfectante de manos, mascarillas, guantes y respiradores. En cambio, lo que las grandes tecnológicas pueden ofrecer son aplicaciones y vigilancia. No es que se haya dado la feliz coincidencia de que, viviendo en la era de la economía de la vigilancia, una app fuera justo lo que necesitábamos en esa situación. Posiblemente se trató, más bien, de que las grandes tecnológicas tienen un tipo de «solución» que buscan imponer a cualquier problema o, como dicen en inglés, son como martillos en busca de clavos.

Tal vez se diera prioridad a las aplicaciones porque las tecnologías están envueltas en un aura de pensamiento mágico, una esperanza de que puedan resolver de forma milagrosa todos nuestros problemas. Tal vez se debiera a que existen incentivos económicos para la recopilación de datos. Tal vez fuera

porque los gobiernos no tenían ni idea de cómo resolver la crisis, y aceptar los múltiples ofrecimientos de apps que recibieron fue una salida fácil para mostrar a la ciudadanía que estaban haciendo *algo* . (Que ese algo no sirviera de mucho es otra historia.) Tal vez fue una combinación de factores. El caso es que ninguna aplicación puede sustituir a lo que de verdad necesitábamos para solucionar nuestros problemas médicos: pruebas diagnósticas, un buen sistema de apoyo a las personas que necesiten aislarse, equipos de protección y vacunas para prevenir la infección, así como medicinas y otros recursos para tratar a los pacientes. Ni las apps son varitas mágicas, ni tener más datos y menos privacidad es la solución a todos nuestros problemas.

La pandemia de 2020 no ha sido la primera situación de emergencia que ha puesto en riesgo la privacidad, y tampoco será la última. Tenemos que aprender a manejar mejor este tipo de escenarios. «Nunca desperdicies una crisis grave —dijo una vez Rahm Emanuel, jefe de gabinete de la Casa Blanca con Barack Obama—, [pues es una] oportunidad de hacer cosas que hasta entonces pensabas que no podías hacer.» [92] En su libro *La doctrina del shock* , Naomi Klein documenta ampliamente casos de desastres que se han aprovechado como oportunidades para impulsar iniciativas políticas extremas que aumentaron los poderes del Estado. [93] Cuando sobreviene una crisis, los ciudadanos se desorientan, se distraen con aquello que es urgente, se asustan y están más a merced de sus dirigentes. Con demasiada frecuencia, ese termina siendo un cóctel nocivo para la democracia. Se aprovechan circunstancias extraordinarias para imponer nuevas normalidades que la ciudadanía jamás habría tolerado en tiempos menos excepcionales. Y pocos cambios son tan duraderos como los introducidos con la pretensión de que sean solamente provisionales.

No hay que olvidar que así fue como llegamos a donde estamos. Aceptamos medidas extraordinarias a raíz del 11-S, y esas medidas todavía nos persiguen. En China, se utilizaron acontecimientos como los Juegos Olímpicos de Pekín de 2008 y la Exposición Universal de 2010 para introducir una vigilancia que se mantuvo una vez finalizados los eventos. [94] Algunas de las medidas de vigilancia que se impusieron para controlar el coronavirus en algunos países fueron draconianas, y los ciudadanos tienen razón en temer su persistencia. Debemos estar muy atentos a cómo se usan nuestros datos. Ya se han producido abusos con los datos de seguimiento y rastreo. En Reino Unido, por ejemplo, se han vendido a terceros datos de rastreo de contactos recogidos en pubs y restaurantes (datos que se suponía que se usarían solo a efectos de salud pública). [95]

Los gigantes tecnológicos no están dejando pasar la oportunidad de ampliar el alcance de su injerencia en nuestras vidas. No se trata solo de apps de rastreo de

contactos. El confinamiento se usó a modo de laboratorio con el que experimentar un futuro muy lucrativo sin contacto. [96] La vigilancia digital está ganando terreno en el entretenimiento, el trabajo, la educación y la salud. Multimillonarios de las nuevas tecnologías como Eric Schmidt están presionando para que se cierren «acuerdos de colaboración sin precedentes entre el Estado y el sector privado». [97] Palantir, la compañía respaldada por la CIA que ayudó a la Agencia de Seguridad Nacional (NSA) a espiar a todo el mundo, colabora ahora tanto con el Servicio Nacional de Salud (NHS) británico [98] como con el Departamento de Salud y Servicios Humanos y los Centros para el Control y la Prevención de Enfermedades en Estados Unidos. [99] El NHS facilitó a Palantir datos de todo tipo acerca de pacientes, empleados y ciudadanos en general: desde información sobre contactos hasta detalles sobre su género, su raza, su trabajo, su estado de salud física y mental, su afiliación política y religiosa, así como sus antecedentes penales. [100]

Hay quienes esperan que la pandemia provoque una reactivación del Estado del bienestar y de la solidaridad de un modo muy parecido a lo que sucedió tras la Segunda Guerra Mundial. Solo que, en esta ocasión, en muchos países las prestaciones sociales están siendo ligadas a empresas privadas y a herramientas y plataformas de vigilancia digital. [101] Secuestrar la ayuda social y pedir por ella un rescate en forma de datos es aprovecharse de los desfavorecidos. En febrero de 2020, un tribunal holandés sentenció que los sistemas de vigilancia de las prestaciones sociales vulneran los derechos humanos, y ordenó el cese inmediato de un programa de detección de fraude en las ayudas. [102] Otros países deberían tomar nota. Los buenos gobiernos no pueden consentir la violación sistemática del derecho fundamental de sus ciudadanos a vivir libres de vigilancia. La privacidad no debe ser el precio que se tenga que pagar por acceder a nuestros demás derechos (como la educación, la sanidad y la seguridad, entre los más destacados).

El coronavirus ha matado a muchos más neoyorquinos que el 11-S. ¿Repetiremos los errores que cometimos entonces? Uno de los peligros de invocar el terrorismo o las epidemias para justificar invasiones de la privacidad es que *esas amenazas nunca van a desaparecer* . El riesgo de que se produzca un atentado terrorista o una epidemia es permanente. Como ya hemos visto, la vigilancia masiva no parece aumentar nuestra seguridad frente al terrorismo. Todavía no está claro si puede ayudarnos a protegernos de las epidemias. Es muy dudoso que lo haga. Pero, incluso si lo hiciera, ¿a qué precio? Si te confinaras en el sótano de tu casa para siempre, estarías bastante a salvo del terrorismo y de las epidemias, pero ¿valdría la pena? ¿Hasta qué punto un pequeño incremento en seguridad compensa la pérdida de derechos civiles? ¿Y no podemos encontrar

formas de aumentar nuestra seguridad sin vulnerar nuestro derecho a la privacidad? Prohibir la cría intensiva o los mercados de animales vivos podría ser mucho más eficaz para prevenir epidemias (por no hablar del potencial beneficio para el bienestar de los animales).

Durante las crisis, es fácil que queramos hacer lo que haga falta para detener la catástrofe que está causando estragos. Pero, además de pensar en cómo frenar un desastre inminente, también debemos tener en cuenta qué mundo nos quedará cuando amaine la tormenta. [103] Por definición, las crisis son pasajeras, pero las políticas que ponemos en práctica tienden a permanecer. Poner fin a un problema ahora utilizando métodos que abran la puerta a conflictos aún más graves en el futuro no es ninguna solución. Antes de renunciar a nuestra privacidad en un contexto de crisis, deberíamos estar del todo seguros de que eso sea necesario, y de que tenemos un modo de recuperar el control de nuestros derechos una vez superada la emergencia. De lo contrario, podríamos terminar en un hoyo más profundo que aquel del que tratábamos de escapar.

AHORA ES EL MOMENTO

Por muy poderosos e irremediables que nos parezcan los gigantes tecnológicos, todavía no es demasiado tarde para reformar el ecosistema de los datos. Son muchas las partes de la economía que todavía no se han digitalizado. En Occidente, antes de la llegada de la pandemia de coronavirus, solo una décima parte de las ventas del comercio minorista se realizaban en línea, y en torno a un quinto del trabajo informático se localizaba en la nube. [104] La pandemia nos ha empujado más hacia el terreno digital. Tenemos que ir con cuidado. Si dejamos que los gigantes tecnológicos continúen expandiéndose sin fijar unas normas estrictas sobre lo que pueden convertir en datos y lo que pueden hacer con esos datos, pronto será demasiado tarde. El momento de actuar es ahora.

6

Lo que puedes hacer

La mayoría de los cambios sociales, económicos, políticos y tecnológicos cruciales que han experimentado las sociedades parecieron en algún momento inconcebibles para la mayoría de la población. Esto es así tanto para las transformaciones positivas como para las negativas: los derechos de las mujeres, la electricidad, las democracias liberales, los aviones, el comunismo, el Holocausto, la catástrofe nuclear de Chernóbil, internet. Todas parecían imposibles. Y, sin embargo, ocurrieron.

El mundo puede cambiar muy rápido y muy a fondo. A principios de marzo de 2020, la rutina diaria en la que vivíamos parecía muy asentada: la gente iba y venía, los supermercados estaban bien abastecidos y los hospitales funcionaban con normalidad. En cuestión de semanas, un tercio de la humanidad pasó a estar confinado por completo por culpa de la pandemia de coronavirus. Gran parte de los viajes internacionales se interrumpieron, ir a comprar comida se convirtió en una excursión arriesgada y, en ocasiones, complicada, y los servicios sanitarios quedaron sobrepasados por el aluvión de casos.

La filosofía budista llama «impermanencia» a la naturaleza cambiante de la vida. El potencial de transformación puede resultarnos amenazador, porque nos recuerda que las cosas pueden empeorar en cualquier momento. Pero la impermanencia también permite que las cosas mejoren y, en particular, nos da la oportunidad de mejorar las cosas nosotros mismos. Todo está condenado a cambiar, y depende de nosotros aprovechar esa realidad fundamental de la vida para hacer todo lo posible por asegurarnos de que los cambios sean para mejor.

La historia de los derechos es, en buena medida, la de un reconocimiento progresivo de que los seres humanos no somos recursos que explotar, sino individuos a quienes respetar. Los derechos laborales son especialmente relevantes en este contexto porque siempre habrá presiones económicas para ignorarlos. Primero reconocimos que todos los seres humanos tienen unos derechos como dueños de sí mismos y que es inaceptable tratar a las personas como si fueran propiedades de otros. Luego reconocimos que los seres humanos tienen derecho a disfrutar de ciertas condiciones básicas de trabajo, como un entorno seguro, una jornada laboral aceptable, un salario adecuado, vacaciones, etcétera.

El que pueda resultar rentable ignorar los derechos de algunas personas es irrelevante: los derechos laborales son derechos humanos que representan líneas rojas que no se pueden traspasar. Para que el capitalismo sea habitable —y compatible con la democracia y la justicia— tenemos que marcarle unos límites. Tenemos que asegurarnos de que las empresas encuentren formas de obtener beneficios que no pasen por la destrucción de aquello que valoramos.

En el pasado, los movimientos sociales han jugado un papel crucial en la aprobación de leyes que reconozcan derechos y mejoren la sociedad. Las prácticas explotadoras terminan en cuanto se las prohíbe por ley, pero somos personas como tú y como yo quienes tenemos que cambiar la cultura para que esas leyes puedan llegar a tramitarse e implementarse. Para cambiar el panorama actual de la privacidad, tenemos que escribir sobre el tema, convencer a otros de que protejan su privacidad y la nuestra, organizarnos, desvelar el funcionamiento interno de ese sistema abusivo que es la sociedad de la vigilancia, apoyar alternativas, idear nuevas posibilidades y negarnos a colaborar con nuestra propia vigilancia.

Todo sistema social depende de que las personas cooperen con él. Cuando las personas dejan de hacerlo, el sistema se descompone. A menudo, la necesidad de cooperación no es evidente hasta que esta cesa y, al hacerlo, toda la maquinaria se detiene. El comercio con datos personales depende de nuestra cooperación. Si dejamos de colaborar con el capitalismo de la vigilancia, podemos cambiarlo. Si buscamos alternativas favorables a la privacidad y optamos por ellas, estas prosperarán.

En este capítulo, encontrarás consejos —desde los más sencillos hasta los más trabajosos— para proteger mejor tu privacidad y la de los demás. No todo el mundo querrá hacer todo lo que pueda por proteger la privacidad. Preservar la seguridad de tus datos personales en esta fase de la era digital puede resultar incómodo. Hasta dónde estés dispuesto a llegar dependerá de lo fuerte que sea tu convicción de que proteger tu privacidad es tu deber, así como de cuáles sean tus circunstancias personales. Si eres un activista que reside en un país poco democrático, es probable que estés dispuesto a hacer mucho por defender tu privacidad. Si vives en un país seguro, tienes un empleo estable y no tienes previsto pedir una hipoteca en un futuro inmediato, tal vez te muestres menos estricto. Tú eliges. Sin embargo, antes de tomar una aproximación demasiado permisiva en cuanto a tu privacidad, ten en cuenta los tres factores siguientes.

En primer lugar, la comodidad está sobrevalorada, por muy tentadora que sea. La comodidad, como el placer, es un componente importante de una vida buena; nos permite una vida más fácil. Si no optáramos por la comodidad de vez en cuando, nuestras vidas se volverían desesperantemente inconvenientes e

ineficientes. Pero la comodidad también es peligrosa. Nos lleva a tener estilos de vida sedentarios, a consumir comida basura, a apoyar a empresas que perjudican a la sociedad, a seguir rutinas diarias monótonas e insatisfactorias, a ser incultos y políticamente apáticos. Hacer ejercicio, leer, aprender, inventar nuevos modos de vivir e interactuar, y luchar por causas justas son actividades tan inconvenientes como significativas. Los logros más gratificantes en la vida rara vez son aquellos que menos cuesta conseguir. Una vida buena exige un grado razonable de lucha: un equilibrio adecuado entre la facilidad de la comodidad y los beneficios del esfuerzo significativo. Como el placer, la comodidad ha de sopesarse con el precio que tenemos que pagar por ella, y con las consecuencias probables a las que da lugar. [1]

En segundo lugar, las decisiones que tomes hoy determinarán el grado de privacidad con el que cuentes en el futuro. Aunque pienses que ahora mismo no tienes nada que ocultar, puede que sí lo tengas dentro de unos años, y entonces podría ser demasiado tarde (los datos ya cedidos a menudo no se pueden retirar). Puede que tu país sea respetuoso con tus derechos humanos en la actualidad, pero ¿puedes estar seguro de que seguirá siéndolo dentro de cinco o diez años?

En tercer lugar, qué tanta privacidad tengas influye en el nivel de privacidad de tus seres queridos, tus conocidos, tus conciudadanos y las personas que se te parecen. La privacidad es algo colectivo y político; no se trata solo de ti.

Con estas advertencias en mente, he aquí algunas cosas que puedes hacer para proteger mejor la privacidad.

PIÉNSATELO DOS VECES ANTES DE COMPARTIR

Eres uno de los mayores riesgos para tu propia privacidad. Los seres humanos son seres sociables y muchas plataformas digitales como Facebook están diseñadas a propósito para que nos sintamos en ellas como en nuestra sala de estar. Pero, a diferencia de lo que ocurre en nuestra sala de estar (cuando está libre de tecnologías digitales), en línea hay una infinidad de empresas y de agencias gubernamentales que nos escuchan. La próxima vez que publiques algo, pregúntate cómo podría usarse en tu contra. Y deja volar la imaginación, porque a veces hace falta ingenio para figurarte el mal uso que se puede hacer de tu información privada o de tus fotografías. Por ejemplo, la mayoría de las personas no se lo piensan antes de publicar una foto en la que se puede ver parte de las manos o los dedos. Pero es posible leer (e incluso clonar) unas huellas digitales a partir de una fotografía. [2] Ten presente que las fotos también contienen metadatos sobre la ubicación, la hora y la fecha. Haz una búsqueda

sobre cómo borrar esa información de tus fotos antes de subirlas a cualquier sitio (el método exacto varía según el dispositivo). Por lo general, cuanto menos compartas en línea, mejor. A veces, lo que quieres compartir es lo bastante importante como para que el riesgo merezca la pena, pero no compartas sin pensar.

Respeta la privacidad de otros

Respeta los derechos de otras personas. Antes de publicar la fotografía de otra persona, pídele su consentimiento. Así, será más probable que otros te pidan permiso la próxima vez que les apetezca publicar algo sobre ti. En tiempos más ingenuos, la mayoría de la gente pensaba que era suficiente contar con la posibilidad de «desetiquetarse» de fotos colgadas por otros. Ahora sabemos que el reconocimiento facial puede utilizarse para identificarte, con o sin etiqueta.

Si alguien te saca una foto o te graba sin tu consentimiento, no dudes en pedirle que no publique ese contenido en línea. Cuando empecé a preocuparme por la privacidad, me daba reparo pedir esas cosas. Pero las respuestas que he recibido desde entonces me han convencido de que la mayoría de la gente empatiza con la preocupación por la privacidad. Para mi sorpresa, la mayoría no solo no se molestan ni tampoco se muestran indiferentes ante mis solicitudes de privacidad, sino que sienten curiosidad por mis razones y se extrañan de que nunca se les haya ocurrido antes que compartir fotografías de otras personas sin antes pedirles permiso podría ser desconsiderado. A medida que las personas van concienciándose más de los riesgos asociados a compartir información en línea, se va haciendo más habitual pedir consentimiento antes de publicar algo en las redes sociales.

Cuando invites a alguien a casa, adviértele de los dispositivos inteligentes que tengas. Incluso el director de *hardware* de Google, Rick Osterloh, lo recomendó cuando le preguntaron por ello en un acto. «Uf, nunca había pensado sobre esto de ese modo», dijo. Ahí tienes una muestra de lo inconscientes que pueden ser los diseñadores de tecnologías a propósito de la privacidad y de nuestro bienestar en general. Por lo menos, Osterloh fue sincero y admitió que los dueños de altavoces inteligentes deberían informar de estos a sus invitados. [3] Eso es más de lo que se puede decir de muchos peces gordos de las compañías tecnológicas.

Tus invitados no son los únicos que merecen privacidad: también se les debe a los niños. No está bien subir a las redes sociales imágenes de los hijos menores de otras personas sin el permiso de sus padres. Ni siquiera si son tus parientes. [4] Y también deberías respetar la privacidad de tus propios hijos. Los padres de

Sonia Bokhari la tuvieron alejada de las redes sociales hasta que cumplió trece años. Cuando tuvo la edad suficiente para abrirse cuentas en Twitter y en Facebook, descubrió que su madre y su hermana llevaban años compartiendo fotos y relatos sobre ella. Dijo sentirse «totalmente avergonzada y profundamente traicionada». [5] Los niños también son personas (incluso los adolescentes) y tienen derecho a la privacidad. No compartas vídeos de niños a quienes se esté ridiculizando de algún modo, por muy divertidos que sean. Esos niños podrían ser luego objeto de acoso en la escuela por ello, y eso podría cambiar su concepción de sí mismos. Ten cuidado con colgar vídeos graciosos de tus hijos, porque podrían volverse virales.

No te hagas una prueba de ADN por curiosidad. Son tremendamente inexactas y estarás poniendo en riesgo no solo tu propia privacidad, sino también la privacidad genética de tus padres, hermanos, descendientes e innumerables otros parientes durante generaciones.

No traiciones la confianza de las personas. No amenaces con publicar mensajes privados o fotografías de otros para conseguir que hagan lo que tú quieres. Eso se llama chantaje o extorsión, y es ilegal e inmoral. No hagas públicos los mensajes o fotografías privadas de otros. Exponer a otras personas cuando te han dado acceso a su vida privada es una traición y fomenta una cultura de la desconfianza. Tampoco seas cómplice de la exposición de la intimidad. Si alguien te muestra algo que expone la privacidad de otra persona, expresa tu desacuerdo y no lo compartas con otros.

Crea espacios de privacidad

Los espacios en los que podemos gozar de privacidad se han reducido. Necesitamos crear conscientemente zonas de privacidad para recuperar áreas en las que la creatividad y la libertad puedan alzar el vuelo sin impedimentos. Si quieres disfrutar de una fiesta especialmente íntima, pide a tus invitados que no saquen fotos ni graben vídeos, o que no los publiquen en línea. Si quieres que tus alumnos puedan debatir libremente en clase, fija reglas que dejen claro que no se permite a los participantes grabar ni publicar lo que pase en el aula. Si quieres organizar un congreso académico que incentive la exploración de temas controvertidos o de trabajos en curso, apaga cámaras y micrófonos. Deshazte del teléfono cuando pases tiempo con tu familia; déjalo en otra estancia, al menos de vez en cuando. Hay interacciones que difícilmente florecerán bajo vigilancia y que nos perderemos si no les reservamos espacio.

Di «no»

Quizá porque somos seres sociales, parecemos predispuestos a decir «sí» cuando alguien nos pide un favor menor. Cuando alguien te pregunta tu nombre, darlo no parece un gran sacrificio y puede sentirse antisocial decir: «No, lo siento». Esa tendencia a decir «sí» se intensifica en los entornos digitales, cuando se nos pide consentimiento para recopilar nuestros datos personales. Esa notificación de consentimiento se nos hace un estorbo en el camino a lo que nos proponíamos hacer —acceder a un sitio web— y la manera más fácil de librarnos del obstáculo es respondiendo «sí». Hay que estar atento para resistirse a la tentación, pero merece la pena. Las pérdidas de privacidad son como los daños ecológicos o el deterioro de la salud: ningún acto de tirar basura, ninguna calada a un cigarrillo provocará un desastre, pero, la suma de actos lo largo del tiempo sí que podrían causarlo. Cada dato que entregas o retienes importa, aunque no lo parezca.

Algunos sitios web son especialmente reacios a aceptar un «no» por respuesta. En vez de tener un único botón para rechazar la recopilación de datos por parte de todos sus colaboradores, te obligan a decir «no» a cada uno de ellos por separado. Si rechazas las *cookies* , esos sitios web no recuerdan luego las respuestas que diste, por lo que tienes que repetir el proceso cada vez que vuelves a la página. Es irritante e injusto y, si te invade la frustración, cierra ese sitio y busca una alternativa.

Opta por la privacidad

Son muchas las formas en que se nos está arrebatando la privacidad. A veces la falta de privacidad puede parecer inevitable, pero no siempre lo es. Aunque hay prácticas de recogida de datos que son casi imposibles de evitar, a menudo disponemos de más opciones de las que resultan más obvias. Y siempre que tengamos una alternativa, es importante elegir la opción favorable a la privacidad, no solo para proteger nuestros datos personales, sino también para hacer saber a gobiernos y empresas que la privacidad nos importa. Lo que sigue es una lista de cosas que conviene tener presente para proteger tu privacidad cuando compres o uses productos y servicios, así como algunas alternativas a ciertos productos y servicios tan dominantes en el mercado actual como invasivos. El paisaje tecnológico cambia a tal ritmo que es probable que esta lista no incluya los productos más recientes, así que tal vez te interese hacer una búsqueda rápida de las novedades. El mensaje más importante con el que te

debes quedar no es el nombre de unas marcas comerciales determinadas, sino lo que hay que tener en cuenta para proteger mejor tu privacidad.

Dispositivos

Siempre que sea posible, elige dispositivos «tontos» en vez de «inteligentes». Una tetera inteligente no supone necesariamente una mejora con respecto a una tradicional y sí representa un riesgo para la privacidad. Cualquier cosa que pueda conectarse a internet es susceptible de ser jaqueada. Si no necesitas que te oigan ni te vean, elige productos que no tengan cámaras ni micrófonos incorporados.

Piénsatelo bien antes de comprar un asistente digital como Alexa o Google Home. Al introducir micrófonos en tu casa, puede que estés destruyendo la intimidad que tienes con tus seres queridos. Si ya posees uno de estos asistentes, puedes desconectarlo (son magníficos como pisapapeles). Si decides quedarte uno de esos espías, asegúrate de estudiar bien sus opciones de configuración y elegir las de mayor privacidad.

Es especialmente importante escoger bien al comprar portátiles y teléfonos inteligentes. Estos aparatos tienen cámaras y micrófonos, se conectan a internet y guardan gran parte de nuestra información más privada —todas razones de peso para elegir un producto fiable. Antes de escoger un dispositivo, piensa en el país de origen y en los conflictos de intereses que los fabricantes podrían tener (por ejemplo, si la principal vía de ingresos del fabricante de un móvil es a través de la explotación de datos personales, cómprate un móvil distinto).

También ayuda estar al día de las últimas noticias sobre privacidad. En 2018, los directores de la CIA, el FBI y la NSA desaconsejaron a los estadounidenses la compra de aparatos de las compañías chinas Huawei y ZTE porque se sospechaba que sus productos incluían puertas traseras controladas por el Gobierno asiático. [6] En 2019, en un estudio de más de 82.000 apps preinstaladas en más de 1.700 dispositivos Android fabricados por 214 marcas diferentes, se descubrió que estos teléfonos son increíblemente inseguros. [7] Las aplicaciones preinstaladas son software que recibe un trato de favor del fabricante y que puede ser muy difícil de eliminar si no se es un usuario experto; esas apps podrían estar recopilando tus datos y enviándolos a terceros sin tu consentimiento. A menos que seas un *techie* versado en crear un escudo de privacidad para tu teléfono, probablemente lo mejor sea que te alejes de los Android. Y no conserves ninguna aplicación que no necesites: la seguridad de tu teléfono es tan resistente como tu app más vulnerable.

Aplicaciones de mensajería

Lo más importante en las apps de mensajería es que ofrezcan cifrado de extremo a extremo, y que tengas un mínimo de confianza de que el proveedor no hará un mal uso de tus metadatos, ni almacenará mensajes en la nube de forma insegura. Aunque WhatsApp proporciona ese tipo de cifrado, el que sea propiedad de Facebook hace que entren en juego ciertos riesgos para la privacidad. Después de que Facebook la adquiriera, Brian Acton, uno de los cofundadores de la aplicación, lo reconoció: «He vendido la privacidad de mis usuarios». [8]

La opción más segura desde el punto de vista de las amenazas externas es probablemente Signal. Una de mis funciones favoritas de esta aplicación es la posibilidad que ofrece de fijar fechas de caducidad para los mensajes; puedes configurarlos para que desaparezcan después de que los destinatarios los hayan leído. Telegram también merece una mención. Tiene la ventaja de que, cuando eliminas un mensaje, puedes borrarlo de todos los teléfonos (y no solo del tuyo) en cualquier momento, y esa es una función fantástica para protegerte de las amenazas internas. A veces te das cuenta de que no deberías haber enviado algo, o de que confiaste en alguien que no era merecedor de tu confianza. La posibilidad de retirar nuestros mensajes a nuestra voluntad es algo que toda app de mensajería nos debería ofrecer. Sin embargo, Telegram tiene dos desventajas importantes. La primera es que los criptógrafos tienden a desconfiar de su cifrado; probablemente sea menos seguro que el de Signal. [9] Además, las conversaciones no se cifran por defecto; tienes que elegir la opción de «chat secreto». Tanto Signal como Telegram son apps gratuitas y fáciles de usar. Te sorprenderá descubrir cuántos de tus contactos tienen ya instalada alguna de estas alternativas. Y a quienes no las tengan, pídeles que se las instalen. Muchas personas estarán encantadas de disponer de una aplicación de mensajería más segura.

Correo electrónico

Los correos electrónicos son muy inseguros. Un email puede parecernos tan privado como una carta, pero es más bien como una postal sin sobre. No uses el correo electrónico de tu empresa para fines que no tengan que ver con tu trabajo (y, en ocasiones, ni siquiera para eso). Tu jefe puede acceder a tus emails de la cuenta corporativa y, si trabajas en una institución pública, tu correo electrónico puede ser objeto de solicitudes de libertad de información. Para escoger un proveedor de correo electrónico, busca que ofrezca ventajas en materia de privacidad, como facilidad de cifrado, y ten en cuenta el país en el que tiene su

sede central. En estos momentos, Estados Unidos tiene menos restricciones legales con respecto a lo que las compañías pueden hacer con tus datos. Entre las opciones que podría valer la pena estudiar están ProtonMail (Suiza), Tutanota (Alemania) y Runbox (Noruega). Si eres paciente y tienes conocimientos de tecnología, puedes utilizar PGP (Pretty Good Privacy) para cifrar tus correos.

No facilites tu dirección de correo electrónico a todas las empresas y personas que te la pidan. Recuerda: los correos electrónicos pueden contener rastreadores. Si te piden tu cuenta de correo en una tienda, lo normal es que puedas negarte amablemente a darla. Si el dependiente te informa de que necesitan un email para efectuar la venta, dale uno falso; se lo merecen (véase más sobre tácticas de ofuscación un poco más abajo). Para dejar claro por qué lo hago, muchas veces facilito una cuenta de correo electrónico como <noesasuntotuyo@privacidad.com>.

Si te ves obligado a compartir tu dirección de email porque tienes que recibir un mensaje y hacer clic en el enlace que te manden, prueba a usar una cuenta alternativa que contenga la mínima información personal posible para cuando tengas que tratar con interlocutores poco fiables. Para eludir el mayor número de rastreadores posible, busca la opción de configuración de tu proveedor de correo que bloquea todas las imágenes por defecto. Otra buena técnica en ese sentido es la del «email con truco». Supongamos que la dirección de correo electrónico que te has abierto para tratar con los mensajes comerciales basura es <miemail@email.com>. Cuando una compañía pesada te pida tu cuenta, dásela, pero añadiéndole un nombre que permita identificar a esa empresa con facilidad: <miemail+compañíapesada@email.com>. Recibirás el mensaje igualmente, pero podrás bloquear esa dirección si la empresa se pone demasiado pesada y, además, si alguna vez se filtra el email, sabrás quién ha sido el culpable. [10] Quizá lo más seguro sea usar un alias diferente para cada app o empresa. Tanto Firefox como Apple te permiten crear alias de tu email.

Buscadores

Tus búsquedas en internet contienen una parte importante de la información más delicada que se puede recopilar sobre ti. Tiendes a buscar cosas que no sabes, o que quieres, o que te preocupan. Como consultas cosas que te están pasando por la cabeza en cada momento, tus búsquedas son una ventana a tus pensamientos. Deja de usar Google como buscador principal. Cambia el que tengas por defecto en tus navegadores por otro que no recoja datos innecesarios sobre ti. Entre las mejores opciones para la privacidad están DuckDuckGo y Qwant. Siempre

puedes volver a usar Google de manera puntual si te está costando encontrar alguna cosa, pero, según mi experiencia, eso cada vez es menos necesario (de hecho, muchas veces DuckDuckGo es mejor que Google). Para buscar a través de Google sin que se recolecten tus datos, usa Startpage.

Navegadores

Si quieres limitar la cantidad de información que se puede vincular a tu perfil, una buena idea es usar un navegador diferente para cada tipo de actividad. Los distintos navegadores no comparten *cookies* entre sí. (Una *cookie* es ese pequeño paquete de datos que envían los sitios web que visitas y que tu navegador guarda en tu ordenador.) Los sitios web usan *cookies* de autentificación para reconocerte cuando vuelves a visitarlos. A menudo se utilizan también *cookies* de rastreo para recopilar tu historial de navegación, de modo que los anunciantes sepan qué mostrarte. Escoge un navegador con el fin de aquellos sitios web que te obligan a iniciar sesión, y otro para navegar por la red. Brave es un navegador que se ha diseñado teniendo muy presente la privacidad. Una de sus numerosas ventajas es que trae incorporado un bloqueador de anuncios y de rastreadores; además, es más rápido que otros navegadores. Vivaldi y Opera son también buenas opciones. También lo son Firefox y Safari, si se les instalan las extensiones adecuadas. Firefox tiene una característica, los contenedores multicuentas, que aísla las *cookies* según los contenedores que tú configures. [11] Los sitios de un contenedor no pueden ver nada de los sitios que hayas abierto en otro diferente. Eso sí, tienes que haber iniciado sesión con una cuenta de Firefox para poder usarlos.

USA EXTENSIONES Y HERRAMIENTAS QUE FAVOREZCAN LA PRIVACIDAD

Las extensiones de privacidad pueden complementar tu navegador. Si este no bloquea rastreadores y anuncios de forma automática, puedes usar alguna extensión que se encargue de hacerlo.

Los bloqueadores de anuncios son fáciles de encontrar e instalar. Actualmente, más o menos el 47 por ciento de los ciudadanos de la red bloquea publicidad. [12] En cuanto disfrutes de la tranquilidad que te proporcionan los bloqueadores, te preguntarás cómo pudiste aguantar tanto tiempo todos esos anuncios molestos que te acosaban todo el rato y te desconcentraban. Usar bloqueadores de anuncios sirve también para enviar un mensaje claro a empresas y gobiernos: no aceptamos este tipo de cultura publicitaria. Si quieres ser justo con las

compañías que se esfuerzan por mostrarte solo anuncios respetuosos (publicidad contextual que respeta tu privacidad y no distrae demasiado), puedes desactivar tu bloqueador para sus sitios.

Privacy Badger, desarrollado por la Electronic Frontier Foundation, puede bloquear anuncios rastreadores y espías. DuckDuckGo Privacy Essentials también bloquea rastreadores, incrementa la protección por cifrado y ofrece una calificación de privacidad (de la A a la F) para que sepas qué tan protegido estás cuando visitas un sitio web. Además de proteger tu privacidad, bloquear los rastreadores también aumenta tu velocidad de navegación. HTTPS Everywhere es otra extensión desarrollada por la Electronic Frontier Foundation y cifra tus comunicaciones con muchos sitios web. Puedes encontrar otras extensiones capaces de borrar tus *cookies* de forma automática cuando cierras una pestaña, o de limpiar tu historial cada cierto número de días.

Ten presente, sin embargo, que también hay extensiones poco fiables. Cambridge Analytica usó extensiones que parecían inofensivas, como calculadoras y calendarios, para acceder a las *cookies* de sesión de usuarios de Facebook, y eso le permitió conectarse a dicha plataforma como si fuera uno de ellos. [13] Antes de instalarte una extensión, haz una búsqueda rápida sobre ella y asegúrate de que es confiable.

Piensa en lo más privado que haces en línea. Para eso, quizá te interese usar Tor, un programa gratuito y de código abierto que te permite ser anónimo en línea. Tor dirige el tráfico de internet a través de una red mundial de miles de repetidores gestionada por voluntarios. Cuando pides acceso a un sitio web a través de Tor, tu solicitud no le llega desde tu dirección IP, sino desde un nodo de salida integrado en el sistema de Tor (como si fuera otro quien entregara tu mensaje). Ese laberinto de retransmisiones dificulta mucho rastrear en qué usuario se originó cada mensaje. Las ventajas son que los sitios web que visitas no ven tu ubicación y que tu proveedor de servicios de internet no ve qué sitios web visitas. La forma más sencilla de usar ese software es mediante el navegador Tor. Este aísla cada sitio web que visitas para que ni los rastreadores ni los anuncios de terceros puedan seguirte allá adonde vayas.

Utilizar Tor tiene algunos inconvenientes. Como los datos pasan por tantos repetidores antes de llegar a su destino, tu navegación se ralentiza. Es posible que algunos sitios web no funcionen igual de bien. Otra desventaja añadida es que puedes atraer una mayor atención de las agencias de inteligencia, pero es posible que ya hayas hecho eso leyendo este libro (o cualquier artículo sobre el tema de la privacidad). [14] Bienvenido al club. Aunque puede que las agencias de inteligencia no vean lo que haces en línea cuando estás usando Tor, saben que lo estás usando. La buena noticia es que, cuanta más gente normal utilice Tor,

menos sospechoso les parecerá este uso a las autoridades. Proteger tu privacidad no es ilegal; es escandaloso que nos hagan sentir como si lo fuera.

Las Virtual Private Networks (VPN), o redes privadas virtuales, también son herramientas útiles para proteger tu privacidad. Una buena VPN puede canalizar tu tráfico de internet a través de una red privada, cifrada y segura. Las VPN son especialmente útiles cuando quieres acceder a internet por medio de una red compartida por muchos usuarios, como la wifi que puedes encontrar en un aeropuerto u otros espacios públicos. Usar una red wifi pública te hace vulnerable a quien la haya instalado y a otras personas que estén conectadas a ella. Usar una VPN te protege de todos, salvo de la compañía encargada de esta, que tiene amplio acceso a tus datos. Asegúrate de que te puedes fiar de quien está detrás de una VPN determinada antes de usarla. No es fácil saber quién es de fiar, pero a veces resulta relativamente fácil saber quién no lo es. No es de extrañar, por ejemplo, que Facebook usara su VPN, Onavo Protect, para recopilar datos personales. [15] Como norma general, si la VPN es gratuita, lo más probable es que tú seas el producto, así que escoge otra.

Cambia tus opciones de configuración

Deberías dar por sentado que todas las configuraciones de todos los productos y servicios son, por defecto, poco amigables con la privacidad. Asegúrate de cambiar tus opciones y adaptarlas al nivel de privacidad que quieras conseguir. Bloquea las *cookies* en tu navegador (o en algunos de tus navegadores) y, en especial, las *cookies* de seguimiento entre sitios. Si optas por una configuración más segura y privada, puede que la funcionalidad de algunas webs quede afectada. Pero piensa que algunos de esos sitios ni siquiera merecen tu visita. Puedes empezar con una configuración estricta e ir modificándola sobre la marcha, según tus necesidades. Valora la posibilidad de utilizar tu navegador en modo de ventana privada (aunque ten en cuenta que esas modalidades de navegación de incógnito solo borran los rastros de tu actividad en línea en tu ordenador; no te protegen del rastreo externo).

Si quieres ser particularmente precavido, comprueba tu configuración una vez al año, pues las compañías cambian sus términos y condiciones continuamente. Las opciones apropiadas para la protección de la privacidad no siempre están agrupadas en un mismo lugar, por lo que encontrarlas puede resultar más difícil de lo que parece. Si te cuesta dar con ellas, recuerda que no es porque seas tonto, sino porque ellos están abusando de su poder. Puede que merezca la pena hacer una búsqueda en línea sobre cómo cambiar tu configuración de privacidad de

ciertos «sospechosos habituales» como Facebook y Google. [16] Con un poco de suerte, tal vez descubras una app que lo haga por ti (Jumbo se presenta como capaz de hacer justamente eso para tu cuenta de Facebook, y puede que se estén desarrollando otras aplicaciones similares).

No acumules demasiados datos

Deshacerse de los datos que ya no necesitas es al entorno virtual lo que la limpieza general es a una casa. [17] Cuantos menos datos almacenes, menos riesgo acumulas. Reconozco que borrar datos es duro. Siempre se tiene la incómoda sensación de que algún día podrían hacernos falta, aunque no los hayas necesitado en una década. En mi caso, una experiencia aleccionadora fue la pérdida hace unos años de buena parte de los datos que guardaba en mi teléfono. En aquel momento, me pareció una catástrofe. Mirando hacia atrás, no los he echado en falta. Una solución menos radical es crear una copia de seguridad de los datos que tienes en línea, guardarla en un disco duro cifrado, y borrarlos de internet. Gracias al Reglamento General de Protección de Datos (RGPD), ahora es más fácil descargarse los datos de las plataformas, aunque no seas europeo. Por ejemplo, es muy sencillo solicitar la descarga de tus datos desde tu cuenta de Twitter, y luego utilizar una app para borrar tus tuits antiguos.

Borrar de verdad la información digital de tus dispositivos es a veces difícil debido a cómo funcionan actualmente los ordenadores. Cuando borras un archivo de tu ordenador, sigue estando ahí, aunque ya no esté a la vista. Los datos no se han tocado. Lo único que ha cambiado es el mapa de archivos del ordenador. El ordenador finge que el archivo ya no está ahí y marca el espacio que ocupaba como un espacio libre. Sin embargo, continúa ahí y por eso se puede usar software de recuperación de archivos. Cualquiera con los conocimientos y la motivación suficientes podría dar con tus ficheros borrados. Si alguna vez quisieras vender tu portátil, por ejemplo, asegúrate de que borras realmente tus archivos. El mejor modo es encriptando tu disco duro (algo que deberías hacer de todos modos) y borrando la clave. Eso lo convierte en crípticamente inaccesible; los datos encriptados parecen un galimatías. [18]

Escoge contraseñas seguras

Nunca uses «123456», ni «contraseña», ni el nombre de tu equipo favorito de fútbol, ni información personal como tu nombre o tu fecha de nacimiento, como clave de acceso. Evita las contraseñas más comunes. [19] La característica más

importante de una contraseña es su longitud. Utiliza claves largas, con letras tanto minúsculas como mayúsculas, caracteres especiales y números. No uses la misma contraseña para todos los sitios. Lo ideal sería que no tuvieras más que una para cada sitio. Puedes utilizar un administrador de contraseñas fiable, capaz de generar claves seguras y recordarlas por ti. Considera la posibilidad de recurrir a la autentificación de múltiples factores, pero ten cuidado a la hora de dar tu número de móvil a empresas que lo vayan a usar para otros fines que no sean exclusivamente tu seguridad. La autentificación ideal con dos factores es una clave física como YubiKey.

UTILIZA LA OFUSCACIÓN

Si un desconocido te para en medio de la calle y te hace una pregunta invasiva, puedes negarte a responderle y marcharte. Internet no te permite permanecer en silencio. Te sigue e infiere información personal sobre ti, lo quieras o no. Es una intromisión equiparable a la de alguien que te pide tu número de teléfono en un bar y se niega a aceptar un «No, gracias» por respuesta. Si esa persona te siguiera acosando para que se lo dieras, ¿qué harías? Tal vez le darías un número falso. Esa es la esencia de la ofuscación.

«La ofuscación es la adición deliberada de información ambigua, confusa o engañosa para interferir en la vigilancia y en la recopilación de datos». [20] En un contexto en el que no te permiten dar el silencio por respuesta, a veces la única forma que tendrás de proteger tu privacidad y protestar es engañar. Por supuesto, las instituciones del Estado, como por ejemplo las autoridades tributarias, tienen un derecho justificado de acceso a parte de tu información personal. Sin embargo, las empresas no siempre tienen tal justificación. Considera la posibilidad de facilitar a compañías a las que no debes dato personal alguno un nombre, una fecha de nacimiento, una dirección de correo electrónico, una ciudad de residencia, etcétera, diferentes de los tuyos. Si quieres manifestar tu protesta al tiempo que practicas la ofuscación, puedes hacerlo escogiendo nombres y direcciones que guarden relación con la privacidad: <miemailesprivado@privacidad.com>, por ejemplo.

Compartir cuentas o dispositivos es otra forma de ofuscar. A un grupo de adolescentes estadounidenses les preocupaba que los gigantes tecnológicos, los administradores de centros escolares, los encargados de admisiones de alumnos de las universidades y los departamentos de personal de distintas empresas pudieran vigilar sus redes sociales. Así que hallaron el modo de proteger su privacidad en Instagram: compartiendo una misma cuenta. Tener una red de

personas que comparten una misma cuenta dificulta que los mirones determinen qué actividad corresponde a cada una de ellas. [21] Compartir dispositivos es incluso mejor para la privacidad, pues así ni siquiera quien estudie detenidamente los datos de una misma cuenta podrá inferir cuáles de ellos corresponden a uno u otro usuario en función del dispositivo desde el que accede.

PÁSATE A LO ANALÓGICO

Minimizar las interacciones digitales es una buena forma de fortalecer la privacidad. Los archivos están probablemente más seguros en papel y guardados bajo llave que en tu ordenador. Siempre que sea posible, paga en efectivo y no con tarjeta de crédito ni con tu teléfono inteligente. Vuelve a los libros en papel; cómpralos en librerías físicas. Déjate el móvil en casa si no lo necesitas. Cuando compres productos, opta por aquellos que no tienen conexión a internet. No necesitas una tetera o una lavadora a través de la que te puedan jaquear. Muy a menudo, lo inteligente es de tontos. [22]

COMPRA PERIÓDICOS

La prensa libre es uno de los pilares de las sociedades libres y abiertas. Necesitamos buen periodismo de investigación, que nos informe de aquello que las empresas y los gobiernos están intentando ocultarnos cuando no deberían hacerlo. Si no fuera por la prensa, tal vez no sabríamos nada sobre el funcionamiento del capitalismo de la vigilancia. Pero, para que la prensa funcione bien, tiene que ser independiente; si es propiedad del poder, corremos el riesgo de que lo sirva a él en vez de a los ciudadanos. Tenemos que pagar por la prensa para que esta trabaje para nosotros. Compra (y lee) diarios y revistas. Mantente bien informado.

La era digital ha sido dura con los periódicos de todo el mundo. Al tener contenidos «gratuitos» en línea, las personas son más reticentes a pagar por una suscripción a un periódico, aunque el contenido sin coste al que terminan accediendo no sea realmente gratuito (tus datos y tu atención son el precio) y su calidad sea cuestionable. Además, el auge de las redes sociales debilitó la relación entre los periódicos y sus lectores. Cuando accedes a la información a través de las redes sociales, es más probable que te veas expuesto a contenidos personalizados y a noticias falsas. Compra periódicos en papel para que nadie pueda rastrear lo que lees. O, como segunda mejor opción, visita los sitios web

de los propios periódicos. Obtén las noticias de la fuente.

EXIGE PRIVACIDAD

Exige que las empresas y las administraciones públicas respeten tus datos. Empecemos por los brókeres de datos. Hay demasiados de ellos como para nombrarlos a todos aquí, pero entre los más grandes destacan Acxiom, Experian, Equifax y Quantcast. Privacy International nos ha simplificado mucho las cosas proporcionándonos modelos de solicitudes y direcciones de correo electrónico a las que enviarlas. [23] También puedes encontrar otra herramienta muy útil para redactar y enviar solicitudes relacionadas con los datos en <mydatadoneright.eu>.

Te lo advierto de antemano: ponerte en contacto por correo electrónico con todas las compañías que tienen tus datos es un suplicio. Muchas veces te ponen las cosas difíciles; tardan mucho en responder, te piden más datos (no se los des si no te parece razonable), pueden mostrarse evasivas. Persevera todo lo que tu paciencia y circunstancias permitan. Puedes enviar esos emails mientras haces cola en la parada del autobús o en el supermercado. Y sé consciente de que puede que no tengas éxito, pero no dejes que eso te desanime. Lo más importante es presentar la solicitud; hace que las compañías tengan que trabajar en ello (imagínate si todos les pidiéramos nuestros datos) y les deja claro que el público no está de acuerdo con sus prácticas. Genera un rastro documental de pruebas que los responsables políticos pueden usar luego para multar y regular a los buitres de datos. Como mínimo, pide tus datos a las empresas que tienen más datos (o datos más sensibles) tuyos.

Exígele privacidad a todo profesional con el que interactúes y te pida tus datos. Haz preguntas. Ten cuidado con tus datos médicos. No uses aplicaciones de salud innecesarias, pues lo más probable es que hagan negocio vendiendo tus datos. Pregunta a tu médico, a tu dentista o a cualquier otro profesional sanitario cuáles son sus prácticas en relación con la privacidad. Diles que no das tu consentimiento para que compartan tus datos.

Para exigir privacidad a las empresas y a los gobiernos, es importante conocer tus derechos. Estúdiate las leyes. Si eres ciudadano europeo, tienes derecho, entre otras cosas, a que se te informe, a acceder a tus datos y corregirlos, a pedir que se borren, a limitar el procesamiento de estos y a llevarte esos datos a otra compañía. Si tienes una queja y no has obtenido solución a un problema que estás teniendo con una compañía y que está relacionado con la privacidad, puedes contactar con tu autoridad nacional de protección de datos, o con el

Supervisor Europeo de Protección de Datos (dependiendo de la naturaleza de la queja). En México, la autoridad correspondiente es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). De poco valen los derechos si solo existen sobre el papel. Tenemos que insuflarles vida.

Ponte en contacto con tus representantes políticos. Envíales un correo electrónico, llámalos. Inclúyelos en tus tuits sobre privacidad. Diles que sientes preocupación por lo que sucede con tus datos personales. Pregúntales qué planes tienen para proteger tu privacidad. Vota a los candidatos adecuados. Cuando unos políticos vulneran tu derecho a la privacidad durante las campañas electorales, te están dando una señal de alerta —no se merecen tu voto.

Si una compañía te decepciona por sus malas políticas de privacidad, expresa una opinión negativa sobre ella en sitios web como Trustpilot, y asegúrate de mencionar la privacidad como motivo en tu queja.

NO DEPENDAS DE ELLAS

Depender de cualquier compañía tecnológica es peligroso. Significa que parte de tu identidad está en sus manos y que, si cancelan tu cuenta o borran tus correos electrónicos (y esas cosas ocurren), puedes tener mucho que perder. Las tecnológicas quieren que dependas de ellas, por lo que es muy difícil no hacerlo. A veces resulta imposible; pero tenlo en cuenta. Hay diferentes grados de dependencia y, cuanto menos dependas de una plataforma o de una aplicación, menos poder tendrán sobre ti. Asegúrate de que, por ejemplo, tienes tus contactos guardados en más de un sitio (preferiblemente, en papel). Mantén vivas tus relaciones con otras personas por más de una vía, para que así, si llega el momento, puedas cerrar tu cuenta en cualquier plataforma sin que esto te suponga una pérdida excesiva.

¿TRABAJAS EN EL SECTOR TECNOLÓGICO?

Tal vez trabajas en alguna de las grandes empresas tecnológicas. O quizá en alguna pequeña *startup* . A lo mejor estás diseñando tu propia aplicación. Sea como fuere, si formas parte del personal dedicado a construir nuestra arquitectura digital, puedes desempeñar un gran papel integrando la privacidad en tus productos desde el principio.

Además de pensar en la rentabilidad, quienes diseñáis tecnología os deberíais preguntar cómo queréis pasar a la posteridad. ¿Quieres que se te recuerde como

una de las personas que ayudaron a empresas y gobiernos a violar el derecho de los individuos a la privacidad, o que puso en riesgo los datos de los usuarios hasta que sucedió una desgracia? ¿Quieres que se te considere una de las personas que contribuyó a quebrar la democracia? ¿O prefieres que se te recuerde como una de las que ayudó a arreglar el ecosistema de los datos ofreciendo a los ciudadanos un modo de navegar por la vida en la era digital sin renunciar a la privacidad?

Uno de los relatos más escalofriantes de cómo una compañía tecnológica puede situarse del lado equivocado de la historia es el libro *IBM y el Holocausto* , de Edwin Black. [24] En él se cuenta cómo IBM contribuyó al genocidio nazi con su sistema de tarjetas perforadas (como ya comenté en el capítulo 4). Las tarjetas perforadas eran una tecnología muy potente, pues aumentaron la capacidad de los estados para controlar a las personas mediante su categorización y contabilización. Pero no se acerca ni por asomo al poder de las tecnologías que hoy se están desarrollando. El reconocimiento facial y las inferencias a partir de macrodatos pueden facilitar un grado de control sobre las personas mucho más poderoso que lo que hemos conocido en el pasado. Leer ese libro me hizo desear que nuestros nietos y bisnietos no tengan que leer algo parecido sobre una de nuestras empresas tecnológicas actuales y su colaboración con algún régimen criminal futuro. [25] Si las compañías tecnológicas quieren estar del lado correcto de la historia, harían bien en proteger nuestra privacidad. La privacidad, además de representar una oportunidad de negocio, es también una oportunidad moral.

Las empresas y los gobiernos están formados por individuos y, aunque algunas personas tienen más poder que otras para conducir una organización por una senda o por otra, todas son moralmente responsables de lo que aportan a sus respectivas instituciones. Los programadores y los diseñadores de tecnologías son especialmente importantes en la era digital. Tienen la habilidad de hacer que las máquinas nos obedezcan. Hacen que la magia se haga realidad. Las instituciones codician a los informáticos, ingenieros y analistas de datos, por lo que estos están muy bien situados para negociar sus responsabilidades. Si trabajas en tecnología y sospechas que colaboras en un proyecto que podría perjudicar a la sociedad, considera presionar a tu jefe para que opte por proyectos más éticos, o incluso dejar ese trabajo y buscarte otro (si te lo puedes permitir).

Los trabajadores del sector tecnológico pueden influir más si disienten en grupo. En 2018, la plantilla de Google logró que la compañía pusiera fin a la política de arbitraje forzado en las denuncias de acoso sexual de los empleados, y que no renovara su contrato para el Proyecto Maven (una colaboración con el

Pentágono). [26] Los disidentes pueden marcar la diferencia. Sigue tu conciencia.

Alfred Nobel se arrepintió de haber inventado la dinamita; Mijaíl Kaláshnikov deseó no haber creado nunca el AK-47; Robert Propst llegó a aborrecer en qué se habían convertido los cubículos de oficina que diseñó; Ethan Zuckerman lamenta haber inventado los anuncios en ventanas emergentes. La lista de inventores que, con el tiempo, renegaron de sus creaciones es muy larga. No te sumes a ella. Las buenas intenciones no bastan; la mayoría de los inventores que se han arrepentido tenían buenas intenciones. Como inventor, tienes que presuponer que alguien intentará hacer un mal uso de tu creación, y tienes que asegurarte de que, por diseño, eso no pueda suceder. Todo un reto.

Si trabajas en el sector tecnológico, puedes buscar asesoramiento en el mundo académico y en las organizaciones sin ánimo de lucro que se preocupan por la privacidad. Seguir la obra de autores como Bruce Schneier, Cathy O'Neil (recomiendo mucho leer su libro, *Armas de destrucción matemática*) o Yves-Alexandre de Montjoye, entre otros, puede aportarte ideas. Organizaciones como la Electronic Frontier Foundation, Privacy International, European Digital Rights y noyb (iniciales en inglés de la frase «no es asunto tuyo») son buenas fuentes de información. Hay algunas consultorías de ética a las que también puedes pedir consejo; asegúrate de que gozan de una buena reputación y de que tienen a alguien realmente formado en ética (parece muy básico, pero no siempre es así). Existen organizaciones que ayudan a las *startups* a despegar y que, como parte de su programa de apoyo, ofrecen una evaluación a cargo de un comité de ética. [27]

Si eres una de esas personas que financia empresas emergentes, asegúrate de exigir a las *startups* en las que inviertas que se sometan a un examen ético de sus productos. Algunas emergentes nunca se preocupan del componente ético de su actividad si no se las incentiva para ello, pues andan demasiado ocupadas en sobrevivir y prosperar, y piensan que la privacidad y la ética son cosas que ya añadirán más tarde al producto final, en cuanto hayan logrado salir adelante. Son muchas las cosas negativas que suceden en el sector tecnológico simplemente porque nadie se paró a pensar qué podría salir mal. La privacidad y la ética tienen que ser requisitos desde el principio de cualquier proyecto tecnológico.

Los diseñadores de tecnología y las empresas preocupadas por la privacidad pueden ejercer una enorme influencia. Moxie Marlinspike y la aplicación de mensajería segura (y sin ánimo de lucro) que creó, Signal, han tenido una inmensa repercusión en nuestra manera de concebir y usar el cifrado. [28] Las nuevas compañías que ofrecen privacidad pueden arrebatar el negocio a las empresas dominantes, y las grandes compañías que mejoran su oferta en

cuestión de privacidad pueden presionar a las demás para que sigan su ejemplo. [29]

HAZ TODO LO QUE PUEDAS

Habla de privacidad con tus amigos y familiares. Tuitea sobre el tema. Si estás en un club de lectura, lee sobre privacidad. En cuanto a obras de ficción, recomiendo *Zed* (de Joanna Kavenna), *El círculo* (de Dave Eggers) y, por supuesto, *1984* (de George Orwell).

Apaga las señales de wifi y *bluetooth* de tu teléfono móvil cuando salgas de casa. Tapa tus cámaras y tus micrófonos con adhesivo. Toma precauciones cuando pases por el control de aduanas en países conocidos por su poco respeto por la privacidad. [30] Estate atento a cualquier oportunidad de proteger tu privacidad. Y hazlo sin esperar alcanzar la perfección.

Todas estas medidas surtirán un efecto. Todas ellas pueden salvarte de violaciones de tu derecho a la privacidad. Pero ninguna es infalible. Es muy difícil tener prácticas de privacidad impecables. Incluso los expertos en el tema cometen deslices con cierta frecuencia. Si estás cansado, tienes prisa o estás distraído, es fácil que des más información de la que querías. Además, si alguien está empeñado en invadir tu privacidad, es probable que termine por conseguirlo.

Aunque no logres proteger tu privacidad a la perfección, siempre debes intentar hacerlo. En primer lugar, puedes conseguir que *algunos* datos personales estén seguros. Eso en sí mismo podría salvarte de un caso de robo de identidad o de exposición de tu intimidad. En segundo lugar, puede que consigas mantener a salvo los datos de otras personas, ya que la privacidad tiene una dimensión colectiva. En tercer lugar, aunque fracasaras en proteger la privacidad, ese tipo de esfuerzos tienen una importante función expresiva: envían el mensaje adecuado. Al exigir que las instituciones protejan nuestra privacidad, estás informando a los políticos y los estás animando a que legislen a favor de la privacidad. Optar por productos respetuosos con la privacidad permite a la industria ver a esta como una ventaja competitiva, una oportunidad de negocio, lo que la animará a innovar a nuestro favor y a dejar de oponerse a la regulación. Los gobiernos y las empresas están más interesados de lo que imaginas por tu opinión sobre la privacidad. Tenemos que dejarles claro lo mucho que nos preocupan nuestros datos personales.

Lo ideal sería que no hiciera falta hacer ninguna de estas cosas, y espero que tus hijos no tengan que tomar tantas precauciones. Igual que es imposible que los

individuos verifiquemos por nuestra cuenta si los ingredientes de todo lo que ingerimos son comestibles —y por ello contamos con organismos reguladores que se encargan de controlarlo—, no menos irrealizable es que los individuos resolvamos los problemas de privacidad a los que nos enfrentamos. Pero sí depende de nosotros motivar a empresas y gobiernos a proteger nuestra privacidad. Podemos conseguirlo. Y para que nuestra cultura comience a preocuparse por la privacidad de nuevo, no hace falta alcanzar la perfección —hacer lo que puedas es más que suficiente.

RECHAZA LO INACEPTABLE

Tomo esta expresión de la autobiografía de Stéphane Hessel, [31] superviviente de un campo de concentración y antiguo miembro de la resistencia francesa que, posteriormente, participó en la redacción de la Declaración Universal de los Derechos Humanos. ¿Qué tienen en común Stéphane Hessel, los abolicionistas, Mahatma Gandhi, Martin Luther King, Rosa Parks, Nelson Mandela, Ruth Bader Ginsburg y todos los demás héroes que han hecho del mundo un lugar mejor? Se negaron a aceptar lo inaceptable. Nuestros héroes no son personas que conviven cómodamente con las injusticias. No aceptan el mundo que se les ha dado cuando es un mundo inaceptable. Son personas que disienten cuando es necesario hacerlo.

Aristóteles sostuvo que, para ser virtuoso, es importante tener emociones apropiadas a las circunstancias. Cuando se viola tu derecho a la privacidad, lo apropiado es sentir indignación moral. No es apropiado sentir indiferencia o resignación.

No te sometas a la injusticia. No pienses que no tienes ningún poder; lo tienes. En el campus central de Microsoft, en Redmond (cerca de Seattle), hay una sala desde la que se gestiona Azure, el servicio de computación en la nube de dicha empresa. Hay allí dos grandes pantallas. En una se muestra el estado del sistema y en la otra se proyecta el «sentimiento» que el sistema despierta en las personas, según lo expresado en las redes sociales. [32] ¿Por qué una compañía como Microsoft iba a preocuparse por lo que las personas sienten acerca de su sistema tanto como por el funcionamiento del propio sistema? Porque lo segundo depende de lo primero. La economía digital en su conjunto depende de ti, de tu cooperación y tu asentimiento. No toleres que violen tu derecho a la privacidad.

La Declaración Universal de los Derechos Humanos es como una carta que nos dejaron quienes nos precedieron; es una advertencia de que nunca debemos cruzar ciertas líneas rojas. Nació del horror provocado por la guerra y el

genocidio. Es una súplica para que no repitamos los errores del pasado. Advierte que las personas se verán compelidas «al supremo recurso de la rebelión» si esos derechos humanos no se respetan. La privacidad es un derecho por muy buenas razones. Defiéndela.

Conclusión

¿En qué tipo de sociedad te gustaría vivir? Hay dos mundos posibles por delante. El primero es una versión más extrema de la sociedad de la vigilancia en la que vivimos hoy. Es un mundo en el que cada paso, cada palabra pronunciada, cada búsqueda en línea, cada compra y cada movimiento del dedo sobre la pantalla de tu teléfono, se registra, se analiza y se comparte con gobiernos y empresas. Drones y satélites te observan desde arriba. El reconocimiento facial te identifica allá adonde vayas. Las autoridades vigilan qué lees y cuándo protestas. La policía, las autoridades de salud pública, las agencias de inteligencia y las compañías de vigilancia reciben esa información. Las autoridades te aseguran que tus datos se usan sobre todo para prevenir pandemias y atentados terroristas. Pero sabes que también se utilizan para mucho más que eso.

La vigilancia no atañe solamente a lo que *haces* , sino también a lo que *piensas* y *sientes* ; es una vigilancia por debajo de la piel. [1] Se escudriña tu cuerpo para inferir tanto tus emociones como tu estado de salud. Por medio de tu reloj, que tal vez estés obligado a llevar puesto por ley, se mide tu frecuencia cardiaca, tu temperatura y tu transpiración. Las empresas de vigilancia emocional registran y analizan aquello que te enfurece cuando estás viendo las noticias, o qué contenido de internet te inspira miedo, y comparten esos datos con las autoridades.

Dicen que esa vigilancia ayuda a la democracia. Dicen que ya no hace falta votar, porque tu Gobierno puede inferir tu opinión política a partir del análisis de datos. Tus datos permiten a los poderosos hacer predicciones sobre tu futuro a partir de las cuales se toman decisiones sobre qué trato te corresponde en tu sociedad. La vigilancia y los algoritmos predictivos deciden si consigues un trabajo, un préstamo o un órgano para un trasplante, si lo necesitas.

Es un mundo en el que las máquinas se ocupan de gestionarte. Si tu frigorífico se está vaciando, encargan la comida que necesitas para mantener tu productividad como miembro de la población activa. Cronometran tu eficiencia en el trabajo, incluidos tus descansos para ir al baño. Te prescriben meditación cuando aumentan tus niveles de estrés. Te dicen cuántos pasos tienes que dar al día como ejercicio para no perder tu acceso a la atención sanitaria.

Es un mundo en el que te preocupa la privacidad de tus hijos. Te preguntas si su futuro puede verse comprometido cuando juegan en línea, pues sabes que sus puntuaciones se venden a brókeres de datos que calculan con ellas sus

capacidades cognitivas. Te preocupa que puedan cometer algún error —como sacarse fotos en plena borrachera adolescente— y que por ello nunca consigan un trabajo. Te preocupa lo obedientes que están obligados a ser si quieren tener una oportunidad en su sociedad. Te preocupa que nunca lleguen a saborear la libertad. Es una sociedad predispuesta para una toma autoritaria del poder.

Afortunadamente, ese no es el único futuro posible que tenemos. Hay un mundo mejor por delante. Uno en el que gobiernos y empresas no sacan partido de lo que es tuyo. Uno en el que los datos en tu teléfono se quedan ahí y nadie tiene acceso a ellos salvo tú. Un mundo en el que nadie puede compartir o vender tus datos, ni siquiera tu familia. Es una sociedad en la que puedes ir al médico y compartir tus síntomas sin preocuparte de que ese acto pueda perjudicarte más adelante. Puedes tener una conversación privada sin que se pueda volver pública. Puedes cometer errores sin que estos definan tu futuro. Puedes buscar en línea lo que te preocupa o lo que te causa curiosidad sin que esos temas de interés se vuelvan luego en tu contra. Puedes buscar el asesoramiento de un abogado sin la sospecha de que el Estado está escuchando y sin temer que lo que digas pueda ser autoincriminatorio. Puedes vivir con la tranquilidad de que la información sobre quién eres, qué has vivido, cuáles son tus esperanzas y miedos, y qué has hecho no se usará en tu contra. Es una sociedad en la que el poder del Gobierno deriva del consentimiento de sus ciudadanos, no de sus datos. Es una sociedad en la que pervive y se perfecciona la milenaria tradición de la democracia.

En un mundo en el que se respeta la privacidad, puedes salir a la calle a manifestarte sin miedo a que te identifiquen. Es un mundo en el que puedes votar en secreto. Puedes explorar ideas desde la intimidad de tu pensamiento y tu hogar. Puedes hacer el amor sin que nadie más que la persona con quien lo haces monitorice tu frecuencia cardiaca, sin que nadie te escuche a través de tus dispositivos digitales. Puedes disfrutar de esa intimidad que solo puede florecer entre personas que saben que nadie más está mirando.

No toda la tecnología es mala. Un mundo en el que podamos disfrutar de privacidad no tiene por qué estar desprovisto de tecnología. Simplemente necesitamos la tecnología adecuada, regulada por las normas apropiadas. La buena tecnología no te fuerza a aceptar nada. Está ahí para aumentar tu autonomía, para ayudarte a alcanzar tus propios objetivos y no los de las tecnológicas de turno. La buena tecnología te habla sin rodeos: sin letra pequeña, sin robos de tus datos a escondidas, sin excusas y sin disculpas. La buena tecnología está a tu servicio. *Tú* eres su cliente, y no los anunciantes, los brókeres de datos o los gobiernos. No eres solo un usuario y en ningún caso eres un súbdito, sino un ciudadano que es también un cliente. La buena tecnología

respeta nuestros derechos y nuestras democracias liberales. La buena tecnología protege tu privacidad.

La privacidad está de vuelta, en contra de las voces que alertaron de que la era digital supondría el fin de la privacidad. No nos encontramos ante el fin de la privacidad, sino más bien ante el principio del fin del capitalismo de la vigilancia. Será una batalla feroz que nunca podremos fiarnos de haber ganado de una vez por todas. Los derechos tienen que defenderse a diario. Las líneas rojas que nunca han de traspasarse tienen que repintarse al inicio de cada temporada. Necesitaremos algo de tiempo para recuperar el control de nuestros datos personales. Y tendremos que hacerlo juntos. Pero puede hacerse y se hará. Cuanto antes, mejor, para ahorrarnos riesgos y daños innecesarios.

Hace seis años, cuando le comentaba a alguien que me dedicaba a investigar sobre la privacidad, solía recibir muchas respuestas pesimistas y cínicas: «Ah, entonces haces historia, no filosofía», o «La privacidad ha muerto, hazte a la idea, ahí no hay nada sobre lo que reflexionar». Algo más cordiales eran las respuestas de quienes intentaban ponerme los pies en la tierra y me animaban a buscar un tema de estudio con mejores perspectivas de futuro. En cierto sentido, por aquel entonces, yo era tan pesimista como los demás a propósito de la privacidad; la brutalidad de la economía de los datos no dejaba mucho margen a la esperanza. Pero también era optimista, porque creía que la naturaleza y la escala del robo de datos personales eran tan atroces y peligrosas que aquella situación era insostenible; las cosas solo podían mejorar. Tenía razón y hoy soy aún más optimista. Ahora, cuando hablo de privacidad, la gente reacciona con interés y preocupación.

El viento ha cambiado. Estamos reaprendiendo el valor de la privacidad tras haberlo olvidado durante un tiempo, deslumbrados como estábamos por el auge de la tecnología digital. Después del escándalo de Cambridge Analytica y de haber experimentado en primera o segunda persona casos de humillación pública o de robo de identidad, ahora comprendemos que las consecuencias de la ausencia de privacidad en nuestros días son tan graves como lo eran antes de la llegada de internet. El robo de tus datos puede salirte tan caro como si te robaran la cartera. Y que los brókeres de datos sepan demasiado sobre ti es aún peor que cuando las empresas podían preguntarte en una entrevista de trabajo si planeabas tener hijos. Al menos, en el pasado, tenían que mirarte a la cara y lo que hacían era visible.

Desde el punto de vista político, nunca había sido tan peligroso que nuestra privacidad esté así de comprometida. Nunca habíamos acumulado tantos datos personales sobre los ciudadanos. Y hemos dejado que la vigilancia crezca en un momento histórico en el que los estándares de ciberseguridad son de pena, las

democracias están en crisis y los regímenes autoritarios con buena mano para el jaqueo están en auge. Las empresas de la tecnología digital utilizaron el manto de la invisibilidad de los datos para erosionar nuestra privacidad. Pero ahora conocemos sus trucos. Podemos volver a tomar el control de nuestros datos personales.

Las secuelas de la pandemia de coronavirus supondrán un reto de primer nivel para nuestra privacidad, pero hoy estamos en una mejor posición para afrontarlo que hace unos años. Sabemos más sobre nuestra privacidad y sobre cómo la están explotando; hay una mayor regulación en cuanto a lo que las instituciones pueden hacer con nuestros datos personales, y hay previstas normativas adicionales para regular estos aún mejor, así como una mayor presión para que las compañías tecnológicas se tomen en serio la privacidad. Hace unos años, nadie pensaba que algo como el Reglamento General de Protección de Datos fuese siquiera posible. A pesar de sus defectos, ha representado un paso de gigante en la dirección correcta. Y solo es el principio.

Actualmente estamos siendo testigos de un proceso civilizador similar al que en su día hizo que nuestra vida en el mundo analógico fuera más soportable. La regulación garantizó que la comida que se vendía fuese relativamente segura, que los clientes pudieran devolver los productos defectuosos, que los automóviles incorporaran cinturones de seguridad y que, por ley, las empresas no pudiesen preguntar a ningún candidato en una entrevista de trabajo si tenía previsto tener hijos. El momento presente es crucial si aspiramos a domar al salvaje Oeste de internet. Las reglas básicas que establezcamos ahora para los datos personales determinarán el terreno de la privacidad durante las próximas décadas. Es fundamental que escojamos bien esas reglas. Nos lo debemos a nosotros mismos y se lo debemos a nuestros hijos.

La privacidad es demasiado importante como para dejarla marchitar. Quién eres y qué haces no es asunto de nadie. No eres un producto que haya que transformar en datos con los que alimentar a los depredadores por un precio. No estás a la venta. Eres un ciudadano y se te *debe* privacidad. Es tu *derecho* . La privacidad es nuestro modo de vendarle los ojos al sistema para que nos trate con imparcialidad y justicia. Es el modo de empoderar a la ciudadanía. Es la forma de proteger a los individuos, las instituciones y las sociedades frente a presiones y abusos externos. Es la manera de demarcar un espacio para nosotros mismos en el que podamos relajarnos, relacionarnos con otros, explorar nuevas ideas y formarnos nuestra propia opinión, todo ello en libertad.

Puede parecer radical exigir el fin de la economía de los datos, pero no lo es. Es el *statu quo* el que hace que nos lo parezca. Lo verdaderamente extremo es aceptar un modelo de negocio que depende de la violación masiva de derechos.

La vigilancia generalizada es incompatible con las sociedades libres y democráticas en las que se respetan los derechos humanos. Tiene que desaparecer. No hay que conformarse con nada menos. Los buitres de datos contraatacarán. Las tecnológicas poco éticas se disculparán y dirán que se portarán mejor a partir de ahora, al tiempo que te pedirán más datos personales. Los gobiernos harán frente común con las empresas de la tecnología invasiva y te prometerán más seguridad a cambio de que les facilites tus datos. Los entusiastas de las tecnologías te dirán que no se le puede poner trabas al progreso. Pero ya no nos engañan. Rechaza lo inaceptable. Recupera el control de tus datos personales, y la privacidad prevalecerá.

Bibliografía

Abramowitz, Michael J., «Freedom in the World. Democracy in Crisis», Freedom House, 2018. <https://freedomhouse.org/report/free dom-world/2018/democracy-crisis>.

Ackerman, Evan, «Why You Should Be Very Skeptical of Ring's Indoor Security Drone», IEEE *Spectrum* , 25 de septiembre de 2020.

Ajunwa, Ifeoma, Kate Crawford y Jason Schultz, «Limitless Worker Surveillance», *California Law Review* , 105 (2017).

Alba, Davey, «The US Government Will Be Scanning Your Face at 20 Top Airports, Documents Show», BuzzFeed, 11 de marzo de 2019.

Allard, Jody, «How Gene Testing Forced Me to Reveal My Private Health Information», *Vice* , 27 de mayo de 2016.

Ambrose, Jillian, «Lights Stay On Despite Cyber-Attack on UK's Electricity System», *The Guardian* , 14 de mayo de 2020.

Angwin, Julia, *Dragnet Nation* , Nueva York, Times Books, 2014.

—, Jeff Larson, Charlie Savage, James Risen, Henrik Moltke y Laura Poitras, «NSA Spying Relies on AT&T's "Extreme Willingness to Help"», *ProPublica* , 15 de agosto de 2015.

Associated Press, «Google Records Your Location Even When You Tell It Not to», *The Guardian* , 13 de agosto de 2018.

Balkin, Jack M., «Information Fiduciaries and the First Amendment», *UC Davis Law Review* , 49 (2016).

Bamford, Roxanne, Benedict Macon-Cooney, Hermione Dace y Chris Yiu, «A Price Worth Paying. Tech, Privacy and the Fight against Covid-19», Tony Blair Institute for Global Change, 2020.

Baraniuk, Chris, «Ashley Madison: "Suicides" over Website Hack», BBC News, 24 de agosto de 2015.

Bassett, Laura, «Digital Media Is Suffocating—and It's Facebook and Google's Fault», *The American Prospect* , 6 de mayo de 2019.

Battelle, John, «The Birth of Google», *Wired* , 1 de agosto de 2005.

Baxter, Michael, «Do Connected Cars Pose a Privacy Threat?», *GDPR . Report* , 1 de agosto de 2018.

Beckett, Lois, «Under Digital Surveillance. How American Schools Spy on Millions of Kids», *The Guardian* , 22 de octubre de 2019.

Bell, Emily, «Why Facebook's News Feed Changes Are Bad News for Democracy», *The Guardian* , 21 de enero de 2018.

Bharat, Krishna, Stephen Lawrence y Mehran Sahami, «Generating User Information for Use in Targeted Advertising», 2003.

Biba, Erin, «How Connected Car Tech Is Eroding Personal Privacy», BBC News, 9 de agosto de 2016.

Biddle, Sam, «For Owners of Amazon's Ring Security Cameras, Strangers May Have Been Watching Too», *The Intercept* , 10 de enero de 2019.

—, «How Peter Thiel's Palantir Helped the NSA Spy on the Whole World», *The Intercept* , 22 de febrero de 2017.

—, «In Court, Facebook Blames Users for Destroying Their Own Right to Privacy», *The Intercept* , 14 de junio de 2014.

«Big Tech's $2trn Bull Run», *The Economist* , 22 de febrero de 2020.

Bilton, Nick, «Why Google Glass Broke», *The New York Times* , 4 de febrero de 2015.

Black, Edwin, *IBM and the Holocaust* , Washington, Dialog Press, 2012. [Hay trad. cast.: *IBM y el Holocausto* , Buenos Aires, Atlántida, 2001.]

Bokhari, Sonia, «I'm 14, and I Quit Social Media after Discovering What Was Posted about Me», *Fast Company* , 18 de marzo de 2019.

Bond, Robert M., *et al* ., «A 61-Million-Person Experiment in Social Influence and Political Mobilization»,

Nature , 489 (2012).
Booth, Robert, Sandra Laville y Shiv Malik, «Royal Wedding. Police Criticised for Pre-Emptive Strikes against Protestors», *The Guardian* , 29 de abril de 2011.
Brin, Sergey y Lawrence Page, «The Anatomy of a Large-Scale Hypertextual Web Search Engine», *Computer Networks and* ISDN *Systems* , 30 (1998).
«British Airways Faces Record £183m Fine for Data Breach», BBC News, 8 de Julio de 2019.
Brooke, Siân, y Carissa Véliz, «Views on Privacy. A Survey», *Data, Privacy & the Individual* , Center for the Governance of Change, IE University, 2020.
Brown, Kristen V., «What DNA Testing Companies' Terrifying Privacy Policies Actually Mean», *Gizmodo* , 18 de octubre de 2017.
Brunton, Finn, y Helen Nissenbaum, *Obfuscation. A User's Guide for Privacy and Protest* , Cambridge (Massachusetts), MIT Press, 2015.
Bryant, Ben, «VICE News Investigation Finds Signs of Secret Phone Surveillance Across London», *Vice* , 14 de enero de 2016.
Burgess, Matt, «More than 1,000 UK Schools Found to Be Monitoring Children with Surveillance Software», *Wired* , 8 de noviembre de 2016.
Burr, Christopher, y Nello Cristianini, «Can Machines Read Our Minds?», *Minds and Machines* , 29 (2019).
Carr, Austin, Matt Day, Sarah Frier y Mark Gurman, «Silicon Valley Is Listening to Your Most Intimate Moments», *Bloomberg Businessweek* , 11 de diciembre de 2019.
Caruso, Jay, «The Latest Battleground Poll Tells Us Democrats Are Over-Correcting for 2020—and They Can't Beat Trump That Way», *The Independent* , 5 de noviembre de 2019.
Chen, Angela, «IBM 's Watson Gave Unsafe Recommendations for Treating Cancer», *Verge* , 26 de julio de 2018.
—, y Alessandra Potenza, «Cambridge Analytica's Facebook Data Abuse Shouldn't Get Credit for Trump», *Verge* , 20 de marzo de 2018.
Christman, John, «Autonomy in Moral and Political Philosophy», en Edward N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* , 2015, <https://plato.stanford.edu/entries/autonomy-moral>.
Clifford, Stephanie, y Quentin Hardy, «Attention, Shoppers. Store Is Tracking Your Cell», *The New York Times* , 14 de julio de 2013.
Cockburn, Harry, «The UK 's Strangest Laws That Are Still Enforced», *The Independent* , 8 de septiembre de 2016.
Coldewey, Devin, «Grindr Send HIV Status to Third Parties, and some Personal Data Unencrypted», *TechCrunch* , 2 de abril de 2018.
Cole, David, «We Kill People Based on Metadata», *The New York Review of Books* , 10 de mayo de 2014.
Comisión de Asuntos Digitales, Cultura, Medios y Deporte, «Disinformation and "Fake News". Final Report», Cámara de los Comunes, 2019.
«Covid-19. China's Qingdao to Test Nine Million in Five Days», BBC News, 12 de octubre de 2020.
Cox, Joseph, «CBP Refuses to Tell Congress How It Is Tracking Americans without a Warrant», *Vice* , 23 de octubre de 2020.
—, «I Gave a Bounty Hunter $300. Then He Located Our Phone», *Motherboard* , 8 de enero 2019.
—, «Revealed. Microsoft Contractors Are Listening to some Skype Calls», *Motherboard* , 7 de agosto de 2019.
Criado Perez, Caroline, *Invisible Women. Exposing Data Bias in a World Designed for Men* , Londres, Vintage, 2019. [Hay trad. cast.: *La mujer invisible. Descubre cómo los datos configuran un mundo hecho por y para los hombres* , Barcelona, Seix Barral, 2020.]
Curran, Dylan, «Are You Ready? Here Is All the Data Facebook and Google Have on You», *The Guardian* , 30 de marzo de 2018.
Dance, Gabriel J. X., Michael Laforgia y Nicholas Confessore, «As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants», *The New York Times* , 18 de diciembre de 2018.
Daniel, Caroline, y Maija Palmer, «Google's Goal. To Organise Your Daily Life», *Financial Times* , 22 de

mayo de 2007.
Das, Shanti, y Shingi Mararike, «Contact-Tracing Data Harvested from Pubs and Restaurants Being Sold On», *The Times* , 11 de octubre de 2020.
«The Data Economy. Special Report», *The Economist* , 20 de febrero de 2020.
Davies, Jessica, «After GDPR, *The New York Times* Cut Off Ad Exchanges in Europe—and Kept Growing Ad Revenue», *Digiday* , 16 de enero de 2019.
Davies, Rob, «Former Cambridge Analytica Chief Receives Seven-Year Directorship Ban», *The Guardian* , 24 de septiembre de 2020.
«Democracy Under Lockdown», Freedom House, octubre de 2020, <https://freedomhouse.org/article/new-report-democracy-underlockdown-impact-covid-19-global-freedom>.
De Montjoye, Yves Alexandre, C. A. Hidalgo, M. Verleysen y V. D. Blondel, «Unique in the Crowd. The Privacy Bounds of Human Mobility», *Scientific Reports* , 3 (2013).
—, L. Radaelli, V. K. Singh y A. S. Pentland, «Identity and Privacy. Unique in the Shopping Mall. On the Reidentifiability of Credit Card Metadata», *Science* , 347 (2015).
De Zwart, Hans, «During World War II, We Did Have Something to Hide», *Medium* , 30 de abril de 2015.
Douglas, Thomas, y Laura van den Borre, «Asbestos Neglect. Why Asbestos Exposure Deserves Greater Policy Attention», *Health Policy* , 123 (2019).
Douglas, Tom, «Why the Health Threat from Asbestos Is Not a Thing of the Past», *The Conversation* , 21 de diciembre de 2015.
Dreyfus, Hubert, y Paul Rabinow, *Michel Foucault. Beyond Structuralism and Hermeneutics* , Chicago, The University of Chicago Press, 1982. [Hay trad. cast.: *Michel Foucault. Más allá del estructuralismo y la hermenéutica* , Buenos Aires, Nueva Visión, 2001.]
Dubois, Daniel J., Roman Kolcun, Anna Maria Mandalari, Muhammad Talha Paracha, David Choffnes y Hamed Haddadi, «When Speakers Are All Ears», *Proceedings on 20th Privacy Enhancing Technologies Symposium* , 2020.
Dunn, Will, «Can Nuclear Weapons Be Hacked?», *New Statesman* , 7 de mayo de 2018.
Dwoskin, Elizabeth, «FTC . Data Brokers Can Buy Your Bank Account Number for 50 Cents», *The Wall Street Journal* , 24 de diciembre de 2014.
Dwoskin, Elizabeth, y Tony Romm, «Facebook's Rules for Accessing User Data Lured More than Just Cambridge Analytica», *The Washington Post* , 20 de marzo de 2018.
«Economic Impact of Advertising in the United States», IHS Economics and Country Risk, 2015.
The Economist Intelligence Unit, «Democracy Index 2019. A Year of Democratic Setbacks and Popular Protest», 2019.
Edwards, Douglas, *I'm Feeling Lucky. The Confessions of Google Employee Number 59* , Boston y Nueva York, Houghton Mifflin Harcourt, 2011.
Ellis-Petersen, Hannah, «Facebook Admits Failings over Incitement to Violence in Myanmar», *The Guardian* , 6 de noviembre de 2018.
Endres, Kyle, «Targeted Issue Messages and Voting Behavior», *American Politics Research* , 48 (2020).
Englehardt, Steven, Jeffrey Han y Arvind Narayanan, «I Never Signed Up For This! Privacy Implications of Email Tracking», *Proceedings on Privacy Enhancing Technologies* , 1 (2018).
Esguerra, Richard, «Google CEO Eric Schmidt Dismisses the Importance of Privacy», Electronic Frontier Foundation, 10 de diciembre de 2009.
Eveleth, Rose, «The Biggest Lie Tech People Tell Themselves—and the Rest of Us», *Vox* , 8 de octubre de 2019.
«Facebook Fined £500,000 for Cambridge Analytica Scandal»,BBC News, 25 de octubre de 2018.
Flyvbjerg, Bent, *Rationality and Power. Democracy in Practice* , Chicago, The University of Chicago Press, 1998.
Foroohar, Rana, «Year in a Word. Techlash», *Financial Times* , 16 de diciembre de 2018.
Forst, Rainer, «Noumenal Power», *The Journal of Political Philosophy* , 23 (2015).
Foucault, Michel, *Discipline and Punish* , Londres, Penguin, 1977. [Hay trad. cast.: *Vigilar y castigar* ,

México, Siglo XXI, 1976.]
Fowler, Geoffrey, «The Doorbells Have Eyes. The Privacy Battle Brewing over Home Security Cameras», *The Washington Post* , 31 de enero de 2019.
Franceschi-Bicchierai, Lorenzo, «Russian Facebook Trolls Got Two Groups of People to Protest Each Other in Texas», *Motherboard* , 1 de noviembre de 2017.
Frederik, Jesse, y Maurits Martijn, «The New Dot Com Bubble Is Here. It's Called Online Advertising», *The Correspondent* , 6 de noviembre de 2019.
Frey, Chris, «Revealed. How Facial Recognition Has Invaded Shops—and Your Privacy», *The Guardian* , 3 de marzo de 2016.
«FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook», *FTC Press Release* , 24 de julio de 2019.
Fung, Brian, «How Stores Use Your Phone's WiFi to Track Your Shopping Habits», *The Washington Post* , 19 de octubre de 2013.
Galdon Clavell, Gemma, «Protect Rights at Automated Borders», *Nature* , 543 (2017).
Gamba, Julien, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador y Narseo Vallina-Rodriguez, «An Analysis of Pre-Installed Android Software», *41st* IEEE *Symposium on Security and Privacy* , 2019.
Gan, Nectar, «China Is Installing Surveillance Cameras outside People's Front Doors–and Sometimes inside Their Homes», *CNN Business* , 28 de abril de 2020.
Gaukroger, Cressida, «Privacy and the Importance of "Getting Away with It"», *Journal of Moral Philosophy* , 17 (2020).
Gellman, Barton, *Dark Mirror* , Londres, Bodley Head, 2020.
Gibbs, Samuel, y Alex Hern, «Google at 20. How Two "Obnoxious" Students Changed the Internet», *The Guardian* , 24 de septiembre de 2018.
Glanz, James, y Andrew W. Lehren, «NSA Spied on Allies, Aid Groups and Businesses», *The New York Times* , 21 de diciembre de 2013.
«The Government Uses "Near Perfect Surveillance" Data on Americans», editorial, *The New York Times* , 7 de febrero de 2020.
Graham, Megan, «Facebook Revenue Chief Says Ad-Supported Model Is "under Assault" amid Apple Privacy Changes», CNBC , 6 de octubre de 2020.
Graham, Richard, «Google and Advertising. Digital Capitalism in the Context of Post-Fordism, the Reification of Language, and the Rise of Fake News», *Palgrave Communications* , 3 (2017).
Gralla, Preston, «How to Protect Your Privacy on Facebook», *Verge* , 7 de junio de 2019.
Gramlich, John, «10 Facts about Americans and Facebook», Pew Research Center, 16 de mayo de 2019.
«Grandmother Ordered to Delete Facebook Photos under GDPR », BBC News, 21 de mayo de 2020.
Grassegger, Hannes, «Facebook Says Its "Voter Button" Is Good for Turnout. But Should the Tech Giant Be Nudging Us at All?», *The Observer* , 15 de abril de 2018.
Grauer, Yael, «What Are "Data Brokers", and Why Are They Scooping Up Information about You?», *Motherboard* , 27 de mayo de 2018.
Greenberg, Andy, «A Guide to Getting Past Customs with Your Digital Privacy Intact», *Wired* , 12 de febrero de 2017.
—, «How Hacked Water Heaters Could Trigger Mass Blackouts», *Wired* , 13 de agosto de 2018.
—, «New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction», *Wired* , 12 de septiembre de 2019.
Grothaus, Michael, «Forget the New iPhones. Apple's Best Product Is Now Privacy», *Fast Company* , 13 de septiembre de 2018.
Guimón, Pablo, «"El Brexit no habría sucedido sin Cambridge Analytica"», *El País* , 27 de marzo de 2018.
Hagey, Keach, «Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggest», *The Wall Street Journal* , 29 de mayo de 2019.
Halpern, Sue, «Cambridge Analytica and the Perils of Psychographics», *The New Yorker* , 30 de marzo de 2018.

Hambling, David, «The Pentagon Has a Laser That Can Identify People from a Distance—by Their Heartbeat», MIT *Technology Review* , 27 de junio de 2019.
Hampton, Keith, Lee Rainie, Weixu Lu, Maria Dwyer, Inyoung Shin y Kristen Purcell, «Social Media and the "Spiral of Silence"», Pew Research Center, 2014.
Harari, Yuval, «The World after Coronavirus», *Financial Times* , 20 de marzo de 2020.
Hartzog, Woodrow, y Evan Selinger, «Facial Recognition Is the Perfect Tool for Oppression», *Medium* , 2 de agosto de 2018.
Harvey, Fiona, «Ozone Layer Finally Healing after Damage Caused by Aerosols, UN Says», *The Guardian* , 5 de noviembre de 2018.
Heaven, Douglas, «An AI Lie Detector Will Interrogate Travellers at some EU Borders», *New Scientist* , 31 de octubre de 2018.
Helm, Toby, «Patient Data From GP Surgeries Sold to US Companies», *The Observer* , 7 de diciembre de 2019.
Henley, Jon, y Robert Booth, «Welfare Surveillance System Violates Human Rights, Dutch Court Rules», The *Guardian* , 5 de febrero de 2020.
Hern, Alex, «Apple Contractors "Regularly Hear Confidential Details" on Siri Recordings», *The Guardian* , 26 de julio de 2019.
—, «Apple Whistleblower Goes Public over "Lack of Action"», *The Guardian* , 20 de mayo de 2020.
—, «Are You A "Cyberhoarder"? Five Ways to Declutter Your Digital Life—from Emails to Photos», *The Guardian* , 10 de octubre de 2018.
—, «Facebook Admits Contractors Listened to Users' Recordings without Their Knowledge», *The Guardian* , 14 de agosto de 2019.
—, «Facebook "Dark Ads" Can Swing Political Opinions, Research Shows», *The Guardian* , 31 de julio de 2017.
—, «Facebook Faces Backlash over Users' Safety Phone Numbers», *The Guardian* , 4 de marzo de 2019.
—, «Hackers Publish Private Photos from Cosmetic Surgery Clinic», *The Guardian* , 31 de mayo de 2017.
—, «Netflix's Biggest Competitor? Sleep», *The Guardian* , 18 de abril de 2017.
—, «Privacy Policies of Tech Giants "Still Not GDPR -Compliant"», *The Guardian* , 5 de julio de 2018.
—, «Smart Electricity Meters Can Be Dangerously Insecure, Warns Expert», *The Guardian* , 29 de diciembre de 2016.
—, «UK Homes Vulnerable to "Staggering" Level of Corporate Surveillance», *The Guardian* , 1 de junio de 2018.
Hernández, José Antonio, «Me han robado la identidad y estoy a base de lexatín; yo no soy una delincuente», *El País* , 24 de agosto de 2016.
Hessel, Stéphane, *The Power of Indignation* , Nueva York, Skyhorse Publishing, 2012.
Hicken, Melanie, «Data Brokers Selling Lists of Rape Victims, AIDS Patients», CNN , 19 de diciembre de 2013.
Hill, Kashmir, «Facebook Added "Research" to User Agreement 4 Months after Emotion Manipulation Study», *Forbes* , 30 de junio de 2014.
—, «Facebook Recommended that This Psychiatrist's Patients Friend Each Other», Splinter News, 29 de agosto de 2016.
—, «Facebook Was Fully Aware that Tracking Who People Call and Text Is Creepy but Did It Anyway», *Gizmodo* , 12 de mayo de 2018.
—, «How Facebook Outs Sex Workers», *Gizmodo* , 10 de noviembre de 2017.
—, «I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too», *The New York Times* , 4 de noviembre de 2019.
—, «"People You May Know". A Controversial Facebook Feature's 10-Year History», *Gizmodo* , 8 de agosto de 2018.
—, «Wrongfully Accused by an Algorithm», *The New York Times* , 24 de junio de 2020.
—, y Aaron Krolik, «How Photos of Your Kids Are Powering Surveillance Technology», *The New York*

Times , 11 de octubre de 2019.
Hodson, Hal, «Revealed. Google AI Has Access to Huge Haul of NHS Patient Data», *New Scientist* , 29 de abril de 2016.
Hoffman, Anna Lauren, «Facebook Is Worried about Users Sharing Lessbut It Only Has Itself to Blame», *The Guardian* , 19 de abril de 2016.
Hoffman, David A., «Intel Executive. Rein In Data Brokers», *The New York Times* , 15 de julio de 2019.
Holpuch, Amanda, «Trump's Separation of Families Constitutes Torture, Doctors Find», *The Guardian* , 25 de febrero de 2020.
Hopkins, Nick, y Stephanie Kirchgaessner, «WhatsApp Sues Israeli Firm, Accusing It of Hacking Activists' Phones», *The Guardian* , 29 de octubre de 2019.
«How WhatsApp Helped Turn an Indian Village into a Lynch Mob», BBC News, 18 de julio de 2018.
Hsu, Jeremy, «The Strava Heat Map and the End of Secrets», *Wired* , 29 de enero de 2018.
Hsu, Tiffany, «The Advertising Industry Has a Problem. People Hate Ads», *The New York Times* , 28 de octubre de 2019.
Inspector General de la NSA , «Report on the President's Surveillance Program», 2009.
Isikoff, Michael, «NSA Program Stopped No Terror Attacks, Says White House Panel Member», NBC News, 20 de diciembre de 2013.
Jenkins, Holman W., «Google and the Search for the Future», *The Wall Street Journal* , 14 de agosto de 2010.
Johnson, Bobbie, «Facebook Privacy Change Angers Campaigners», *The Guardian* , 10 de diciembre de 2009.
—, «Privacy No Longer a Social Norm, Says Facebook Founder», *The Guardian* , 11 de enero de 2010.
Johnston, Casey, «Facebook Is Tracking Your "Self-Censorship"», *Wired* , 17 de diciembre de 2013.
Jones, Rupert, «Identity Fraud Reaching Epidemic Levels, New Figures Show», *The Guardian* , 23 de agosto de 2017.
Kaiser, Brittany, *Targeted. My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy* , Londres, HarperCollins, 2019. [Hay trad. cast.: *La dictadura de los datos. La verdadera historia desde dentro de Cambridge Analytica y de cómo el Big Data, Trump y Facebook rompieron la democracia y cómo puede volver a pasar* , Barcelona, HarperCollins, 2019.]
Kaiser, Jocelyn, «We Will Find You.DNA Search Used to Nab Golden State Killer Can Home In on about 60 % of White Americans», *Science Magazine* , 11 de octubre de 2018.
Kang, Cecilia, y Mike Isaac, «Defiant Zuckerberg Says Facebook Won't Police Political Speech», *The New York Times* , 17 de octubre de 2019.
Kang, Cecilia, y Kenneth P. Vogel, «Tech Giants Amass a Lobbying Army for an Epic Washington Battle», *The New York Times* , 5 de junio de 2019.
Kayyem, Juliette, «Never Say "Never Again"», *Foreign Policy* , 11 de septiembre de 2012.
Kelion, Leo, «Google Chief. I'd Disclose Smart Speakers before Guests Enter My Home», BBC News, 15 de octubre de 2019.
Khan, Lina y David E. Pozen, «A Skeptical View of Information Fiduciaries», *Harvard Law Review* , 133 (2019).
Khandaker, Tamara, «Canada Is Using Ancestry DNA Websites to Help It Deport People», *Vice News* , 26 de julio de 2018.
Kim, Tae, «Warren Buffett Believes This Is "the Most Important Thing" to Find in a Business», CNBC , 7 de mayo de 2018.
Kim, Tami, Kate Barasz y Leslie K. John, «Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness», *Journal of Consumer Research* , 45 (2019).
Klein, Naomi, «Screen New Deal», *The Intercept* , 8 de mayo de 2020.
—, *The Shock Doctrine* , Toronto, Random House, 2007. [Hay trad. cast.: *La doctrina del shock* , Barcelona, Paidós, 2007.]
Kleinman, Zoe, «Politician's Fingerprint "Cloned from Photos"by Hacker», BBC News, 29 de diciembre de

2014.
Knoema, «United States of America—Contribution of Travel and Tourism to GDP as a Share of GDP », 2018.
Kobie, Nicole, «Heathrow's Facial Recognition Tech Could Make Airports More Bearable», *Wired* , 18 de octubre de 2018.
Koch, Richie, «Using Zoom? Here Are the Privacy Issues You Need to Be Aware Of», ProtonMail, 20 de marzo de 2020.
Koepke, Logan, «"We Can Change These Terms at Anytime". The Detritus of Terms of Service Agreements», *Medium* , 18 de enero de 2015.
Koerner, Brendan I., «Your Relative's DNA Could Turn You into a Suspect», *Wired* , 13 de octubre de 2015.
Kornbluh, Karen, Adrienne Goldstein y Eli Weiner, «New Study by Digital New Deal Finds Engagement with Deceptive Outlets Higher on Facebook Today than Run-Up to 2016 Election», German Marshall Fund of the United States, 12 de octubre de 2020.
Kosinski, Michal, David Stillwell y Thore Graepel, «Private Traits and Attributes Are Predictable from Digital Records of Human Behavior», *Proceedings of the National Academy of Sciences (PNAS)* , 110 (2013).
Kramer, Alexis, «Forced Phone Fingerprint Swipes Raise Fifth Amendment Questions», *Bloomberg Law* , 7 de octubre de 2019.
Kurra, Babu, «How 9/11 Completely Changed Surveillance in U. S.», *Wired* , 11 de septiembre de 2011.
Lamont, Tom, «Life after the Ashley Madison Affair», *The Observer* , 28 de febrero de 2016.
Lapowsky, Issie, «The 21 (and Counting) Biggest Facebook Scandals of 2018», *Wired* , 20 de diciembre de 2018.
Lecher, Colin, «Strava Fitness App Quietly Added a New Opt-Out for Controversial Heat Map», *Verge* , 1 de marzo de 2018.
Lee, Jennifer, «Postcards From Planet Google», *The New York Times* , 28 de noviembre de 2002.
Lee, Micah y Yael Grauer, «Zoom Meetings Aren't End-to-End Encrypted, despite Misleading Marketing», *The Intercept* , 31 de marzo de 2020.
Levin, Sam, «Tech Firms Make Millions from Trump's Anti-Immigrant Agenda, Report Finds», *The Guardian* , 23 de octubre de 2018.
Levitsky, Steven y Daniel Ziblatt, *How Democracies Die* , Londres, Penguin, 2018. [Hay trad. cast.: *Cómo mueren las democracias* , Barcelona, Ariel, 2018.]
Levy, Steven, *In the Plex. How Google Thinks, Works, and Shapes Our Lives* , Nueva York, Simon & Schuster, 2011.
Liebermann, Oren, «How a Hacked Phone May Have Led Killers to Khashoggi», CNN , 20 de enero de 2019.
Liu, Xiaoxuan, Livia Faes, Aditya U. Kale, Siegfried K. Wagner, Dun Jack Fu, Alice Bruynseels, Thushika Mahendiran, Gabriella Moraes, Mohith Shamdas, Christoph Kern, Joseph R. Ledsam, Martin K. Schmid, Konstantinos Balaskas, Eric J. Topol, Lucas M. Machmann, Pearse A. Keane y Alastair K. Denniston, «A Comparison of Deep Learning Performance against Health-Care Professionals in Detecting Diseases from Medical Imaging. A Systematic Review and Meta-Analysis», *Lancet Digital Health* , 1 (2019).
Lohr, Steve, «Forget Antitrust Laws. To Limit Tech, Some Say a New Regulator Is Needed», *The New York Times* , 22 de octubre de 2020.
Lomas, Natasha, «A Brief History of Facebook's Privacy Hostility ahead of Zuckerberg's Testimony», *TechCrunch* , 10 de abril de 2018.
—, «The Case against Behavioral Advertising Is Stacking Up», *TedCrunch* , 20 de enero de 2019.
Louis, Tristan, «How Much Is a User Worth?», *Forbes* , 31 de agosto de 2013.
Lukes, Steven, *Power. A Radical View* , Londres, Red Globe Press, 2005. [Hay trad. cast.: *El poder: Un enfoque radical* , Madrid, Siglo XXI, 1985.]
Lyngaas, Sean, «Hacking Nuclear Systems Is the Ultimate Cyber Threat. Are We Prepared?», *Verge* , 23 de enero de 2018.
Macintyre, Amber, «Who's Working for Your Vote?», *Tactical Tech* , 29 de noviembre de 2018.

Maclachlan, Alice, «Fiduciary Duties and the Ethics of Public Apology», *Journal of Applied Philosophy* , 35 (2018).
Magalhães, João Carlos y Nick Couldry, «Tech Giants Are Using This Crisis to Colonize the Welfare System», *Jacobin* , 27 de abril de 2020.
Mahdawi, Arwa, «Spotify Can Tell if You're Sad. Here's Why That Should Scare You», *The Guardian* , 16 de septiembre de 2018.
Malin, Bradley y Latanya Sweeney, «Determining the Identifiability of DNA Database Entries», *Proceedings, Journal of the American Medical Informatics Association* , febrero de 2000.
«A Manifesto for Renewing Liberalism», *The Economist* , 13 de septiembre de 2018.
Marantz, Andrew, «Why Facebook Can't Fix Itself», *The New Yorker* , 12 de octubre de 2020.
Marcus, Gary, «Total Recall. The Woman Who Can't Forget», *Wired* , 23 de marzo de 2009.
Matsakis, Louise, «Online Ad Targeting Does Work—as Long as It's Not Creepy», *Wired* , 11 de mayo de 2018.
—, «The WIRED Guide to Your Personal Data (and Who Is Using It)», *Wired* , 15 de febrero de 2019.
Maxmen, Amy, «Surveillance Science», *Nature* , 569 (2019).
Mayer-Schönberger, Viktor, *Delete. The Virtue of Forgetting in the Digital Age* , Princeton (Nueva Jersey), Princeton University Press, 2009.
Mccue, T. J., «47 Percent of Consumers Are Blocking Ads», *Forbes* , 19 de marzo de 2019.
Merchant, Brian, «How Email Open Tracking Quietly Took Over the Web», *Wired* , 11 de diciembre de 2017.
Metz, Rachel, «The Smartphone App That Can Tell You're Depressed before You Know It Yourself», MIT *Technology Review* , 15 de octubre de 2018.
Michel, Chloé, Michelle Sovinsky, Eugenio Proto y Andrew Oswald, «Advertising as a Major Source of Human Dissatisfaction. Cross-National Evidence on One Million Europeans», en Mariano Rojas (ed.), *The Economics of Happiness* , Nueva York, Springer, 2019.
Miles, Tom, «UN Surveillance Expert Urges Global Moratorium on Sale of Spyware», Reuters, 18 de junio de 2019.
Mill, John Stuart, *Collected Works of John Stuart Mill* , University of Toronto Press, 1963.
—, *On Liberty* , Indianápolis, Hackett Publishing Company, 1978. [Hay trad. cast.: *Sobre la libertad* , Madrid, Alianza, 1984.]
Mims, Christopher, «Here Comes "Smart Dust", the Tiny Computers That Pull Power from the Air», *The Wall Street Journal* , 8 de noviembre de 2018.
Mistreanu, Simina, «Life inside China's Social Credit Laboratory», *Foreign Policy* , 3 de abril de 2018.
Molla, Rani, «These Publications Have the Most to Lose from Facebook's New Algorithm Changes», *Vox* , 25 de enero de 2018.
Moore, Barrington, *Privacy. Studies in Social and Cultural History* , Armonk (Nueva York), M. E. Sharpe, 1984.
Mozur, Paul, Raymond Zhong y Aaron Krolik, «In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags», *The New York Times* , 1 de marzo de 2020.
Müller, Martin U., «Medical Applications Expose Current Limits of AI », *Der Spiegel* , 3 de agosto de 2018.
Munro, Dan, «Data Breaches in Healthcare Totaled over 112 Million Records in 2015», *Forbes* , 31 de diciembre de 2015.
Murphy, Erin E., *Inside the Cell. The Dark Side of Forensic DNA* , Nueva York, Nation Books, 2015.
Murphy, Hannah, «Facebook to Ban Ads That Aim to "Delegitimise an Election"», *Financial Times* , 1 de octubre de 2020.
Murphy, Margi, «Privacy Concerns as Google Absorbs DeepMind's Health Division», *The Telegraph* , 13 de noviembre de 2018.
«Myanmar Rohingya. Why Facebook Banned an Army Chief»,BBC News, 18 de agosto de 2018.
Nagel, Thomas, «Concealment and Exposure», *Philosophy and Public Affairs* , 27 (1998).
Nakashima, Ellen y Joby Warrick, «Stuxnet Was Work of US and Israeli Experts, Officials Say», *The*

Washington Post , 2 de junio de 2012.
«Nature's Language Is Being Hijacked by Technology», BBC News, 1 de agosto de 2019.
Naughton, John, «More Choice on Privacy Just Means More Chances to Do What's Best for Big Tech», *The Guardian* , 8 de julio de 2018.
Neff, Gina y Dawn Nafus, *Self-Tracking* , Cambridge (Massachusetts), MIT Press, 2016.
Newman, Lily Hay, «How to Block the Ultrasonic Signals You Didn't Know Were Tracking You», *Wired* , 3 de noviembre de 2016.
Newton, Casey, «How Grindr Became a National Security Issue», *Verge* , 28 de marzo de 2019.
Ng, Alfred, «Google Is Giving Data to Police Based on Search Keywords, Court Docs Show», CNET , 8 de octubre de 2020.
—, «Teens Have Figured Out How to Mess with Instagram's Tracking Algorithm», CNET , 4 de febrero de 2020.
—, «With Smart Sneakers, Privacy Risks Take a Great Leap», CNET , 13 de febrero de 2019.
Nguyen, Nicole, «If You Have a Smart TV , Take a Closer Look at Your Privacy Settings», CNBC , 9 de marzo de 2017.
Nicas, Jack, «The Police Can Probably Break into Your Phone», *The New York Times* , 21 de octubre de 2020.
Noble, Safiya, *Algorithms of Oppression. How Search Engines Reinforce Racism* , Nueva York, New York University Press, 2018.
Ntiva, Inc., «The Default Privacy Settings You Should Change and How to Do It», *Medium* , 18 de julio de 2018.
«The Observer View on the Information Commissioner's Cambridge Analytica Investigation», editorial, *The Observer* , 11 de octubre de 2020.
O'flaherty, Kate, «Facebook Shuts Its Onavo Snooping App–but It Will Continue to Abuse User Privacy», *Forbes* , 22 de febrero de 2019.
Ogilvy, David, *Confessions of an Advertising Man* , Harpenden (Reino Unido), Southbank Publishing, 2013. [Hay trad. cast.:*Confesiones de un publicitario* , Barcelona, Oikos-Tau, 1965.]
O'hara, Kieron, y Nigel Shadbolt, «Privacy on the Data Web», *Communications of the ACM* , 53 (2010).
Oliver, Myrna, «Legends Nureyev, Gillespie Die. Defector Was One of Century's Great Dancers», *Los Angeles Times* , 7 de enero de 1993.
Olson, Parmy, «Exclusive. WhatsApp Cofounder Brian Acton Gives the Inside Story on #DeleteFacebook and Why He Left $850 Million Behind», *Forbes* , 26 de septiembre de 2018.
Orphanides, K. G., «How to Securely Wipe Anything from Your Android, iPhone or PC », *Wired* , 26 de enero de 2020.
Orwell, George, *Fascism and Democracy* , Londres, Penguin, 2020.
—, *Politics and the English Language* , Londres, Penguin, 2013. [Hay trad. cast.: «La política y la lengua inglesa», en *El poder y la palabra. Diez ensayos sobre lenguaje, política y verdad* , Barcelona, Debate, 2017.]
Osborne, Hilary, «Smart Appliances May Not Be Worth Money in Long Run, Warns Which?», *The Guardian* , 8 de junio de 2020.
O'sullivan, Donie y Brian Fung, «Facebook Will Limit some Advertising in the Week before the US Election–but It Will Let Politicians Run Ads with Lies», *CNN Business* , 3 de septiembre de 2020.
Parcak, Sarah, «Are We Ready for Satellites That See Our Every Move?», *The New York Times* , 15 de octubre de 2019.
Parkin, Simon, «Has Dopamine Got Us Hooked on Tech?», *The Guardian* , 4 de marzo de 2018.
Paul, Kari, «Zoom to Exclude Free Calls from End-to-End Encryption to Allow FBI Cooperation», *The Guardian* , 4 de junio de 2020.
—, «Zoom Will Provide End-to-End Encryption to All Users after Privacy Backlash», *The Guardian* , 17 de junio de 2020.
Penney, Jonathon W., «Chilling Effects. Online Surveillance and Wikipedia Use», *Berkeley Technology Law*

Journal , 31 (2016).
Pérez Colomé, Jordi, «Por qué China roba datos privados de decenas de millones de estadounidenses», *El País* , 17 de febrero de 2020.
Peterson, Andrea, «Snowden Filmmaker Laura Poitras:“Facebook Is a Gift to Intelligence Agencies”», *The Washington Post* , 23 de octubre de 2014.
Phillips, Dom, «Brazil’s Biggest Newspaper Pulls Content from Facebook after Algorithm Change», *The Guardian* , 8 de febrero de 2018.
Poole, Steven, «Drones the Size of Bees–Good or Evil?», *The Guardian* , 14 de junio de 2013.
Popper, Karl, *The Open Society and Its Enemies* , Londres, Routledge, 2002. [Hay trad. cast.: *La sociedad abierta y sus enemigos* , Barcelona, Paidós, 2006.]
Poulson, Jack, «Tech Needs More Conscientious Objectors», The *New York Times* , 23 de abril de 2019.
Powles, Julia, «DeepMind’s Latest AI Health Breakthrough Has some Problems», *Medium* , 6 de agosto de 2019.
—, y Enrique Chaparro, «How Google Determined Our Right to Be Forgotten», The *Guardian* , 18 de febrero de 2015.
—, y Hal Hodson, «Google DeepMind and Healthcare in an Age of Algorithms», *Health and Technology* , 7 (2017).
Price, Rob, «An Ashley Madison User Received a Terrifying Blackmail Letter», *Business Insider* , 22 de enero de 2016.
«Privacy Online. Fair Information Practices in the Electronic Marketplace. A Report to Congress», Federal Trade Commission, 2000.
Purdy, Jebediah, «The Anti-Democratic Worldview of Steve Bannon and Peter Thiel», *Politico* , 30 de noviembre de 2016.
Quain, John R., «Cars Suck Up Data about You. Where Does It All Go?», *The New York Times* , 27 de julio de 2017.
Ralph, Oliver, «Insurance and the Big Data Technology Revolution», *Financial Times* , 24 de febrero de 2017.
Ram, Aliya y Emma Boyde, «People Love Fitness Trackers, but Should Employers Give Them Out?», *Financial Times* , 16 de abril de 2018.
—, y Madhumita Murgia, «Data Brokers. Regulators Try to Rein In the “Privacy Deathstars”», *Financial Times* , 8 de enero de 2019.
Ramsey, Lydia y Samantha Lee, «Our DNA is 99.9 % the Same as the Person Next to Us—and We’re Surprisingly Similar to a Lot of Other Living Things», *Business Insider* , 3 de abril de 2018.
Raphael, J. R., «7 Google Privacy Settings You Should Revisit Right Now», *Fast Company* , 17 de mayo de 2019.
«Revealed: Trump Campaign Strategy to Deter Millions of Black Americans from Voting in 2016», Channel 4 News, YouTube, 28 de septiembre de 2020, <https://www.youtube.com/watch?v=KIf5ELaOjOk>.
Revell, Timothy, «How to Turn Facebook into a Weaponised AI Propaganda Machine», *New Scientist* , 28 de julio de 2017.
Rogers, Kaleigh, «Let’s Talk about Mark Zuckerberg’s Claim that Facebook “Doesn’t Sell Data”», *Motherboard* , 11 de abril de 2019.
Romm, Tony, «Tech Giants Led by Amazon, Facebook and Google Spent Nearly Half a Billion on Lobbying over the Last Decade», *The Washington Post* , 22 de enero de 2020.
Rosenberg, Eli, «Quote. The Ad Generation», *The Atlantic* , 15 de abril de 2011.
Rosenberg, Matthew, «Ad Tool Facebook Built to Fight Disinformation Doesn’t Work as Advertised», *The New York Times* , 25 de julio de 2019.
Russell, Bertrand, *Power. A New Social Analysis* , Londres, Routledge, 2004. [Hay trad. cast.:*El poder. Un nuevo análisis social* , Barcelona,RBA , 2010.]
Salinas, Sara, «Six Top US Intelligence Chiefs Caution against Buying Huawei Phones», CNBC , 13 de

febrero de 2018.
Sanger, David E., «Hackers Took Fingerprints of 5.6 Million U. S. Workers, Government Says», *The New York Times* , 23 de septiembre de 2015.
Sanghani, Radhika, «Your Boss Can Read Your Personal Emails. Here's What You Need to Know», *The Telegraph* , 14 de enero de 2016.
Satariano, Adam, «Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates», *The New York Times* , 27 de abril de 2020.
Savage, Charlie, «Declassified Report Shows Doubts about Value of N. S. A.'s Warrantless Spying», *The New York Times* , 24 de abril de 2015.
—, *Power Wars. Inside Obama's Post-9/11 Presidency* , Nueva York, Little, Brown & Company, 2015.
Schilit, S. L. y A. Schilit Nitenson, «My Identical Twin Sequenced Our Genome», *Journal of Genetic Counseling* , 16 (2017).
Schneier, Bruce, *Click Here to Kill Everybody. Security and Survival in a Hyper-Connected World* , Nueva York, W. W. Norton & Company, 2018. [Hay trad. cast.: *Haz clic para matarlos a todos. Un manual de supervivencia* , Barcelona, Temas de Hoy, 2019.]
—, *Data and Goliath* , Nueva York, W. W. Norton & Company, 2016.
—, «Data Is a Toxic Asset, So Why Not Throw It Out?», CNN , 1 de marzo de 2016.
Schneier, Bruce, y James Waldo, «AI Can Thrive in Open Societies», *Foreign Policy* , 13 de junio de 2019.
Schumpeter, «Something Doesn't Ad Up about America's Advertising Market», *The Economist* , 18 de enero de 2018.
Segall, Laurie, «Pastor Outed on Ashley Madison Commits Suicide», CNN , 8 de septiembre de 2015.
Selinger, Evan y Woodrow Hartzog, «What Happens When Employers Can Read Your Facial Expressions?», *The New York Times* , 17 de octubre de 2019.
Seltzer, William y Margo Anderson, «The Dark Side of Numbers. The Role of Population Data Systems in Human Rights Abuses», *Social Research* , 68 (2001).
Shaban, Hamza, «Google for the First Time Outspent Every Other Company to Influence Washington in 2019», *The Washington Post* , 23 de enero de 2018.
Shadbolt, Nigel y Roger Hampson, *The Digital Ape. How to Live (in Peace) with Smart Machines* , Oxford, Oxford University Press, 2019.
Shaer, Matthew, «The False Promise of DNA Testing», *The Atlantic* , junio de 2016.
Sherman, Len, «Zuckerberg's Broken Promises Show Facebook Is Not Your Friend», *Forbes* , 23 May 2018.
Shontell, Alyson, «Mark Zuckerberg Just Spent More than $30 Million Buying 4 Neighboring Houses for Privacy», *Business Insider* , 11 de octubre de 2013.
Singel, Ryan, «Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims», *Wired* , 17 de diciembre de 2009.
Singer, Natasha, «Data Broker Is Charged with Selling Consumers' Financial Details to "Fraudsters"», *The New York Times* , 23 de diciembre de 2014.
—, «Facebook's Push for Facial Recognition Prompts Privacy Alarms», *The New York Times* , 9 de julio de 2018.
Smith, Dave y Phil Chamberlain, «On the Blacklist. How Did the UK 's Top Building Firms Get Secret Information on Their Workers», *The Guardian* , 27 de febrero de 2015.
Smith, David, «How Key Republicans inside Facebook Are Shifting Its Politics to the Right», *The Guardian* , 3 de noviembre de 2019.
Snowden, Edward, *Permanent Record* , Londres, Macmillan, 2019. [Hay trad. cast.: *Vigilancia permanente* , Barcelona, Planeta, 2019.]
Solon, Olivia, «Ashamed to Work in Silicon Valley. How Techies Became the New Bankers», *The Guardian* , 8 de noviembre de 2017.
—, «"Data Is a Fingerprint". Why You Aren't as Anonymous as You Think Online», *The Guardian* , 13 de julio de 2018.

—, «“Surveillance Society”. Has Technology at the US -Mexico Border Gone Too Far?», *The Guardian* , 13 de junio de 2018.
St. John, Allen, «How Facebook Tracks You, even When You’re Not on Facebook», *Consumer Reports* , 11 de abril de 2018.
«Stalker “Found Japanese Singer through Reflection in Her Eyes”», BBC News, 10 de octubre de 2019.
Stanokvic, L., V. Stanokvic, J. Liao y C. Wilson, «Measuring the Energy Intensity of Domestic Activities from Smart Meter Data», *Applied Energy* , 183 (2016).
Statt, Nick, «Facebook CEO Mark Zuckerberg Says the “Future Is Private”», *Verge* , 30 de abril de 2019.
—, «How AT&T ’s Plan to Become the New Facebook Could Be a Privacy Nightmare», *Verge* , 16 de julio de 2018.
—, «Peter Thiel’s Controversial Palantir Is Helping Build a Coronavirus Tracking Tool for the Trump Admin», *Verge* , 21 de abril de 2020.
Stehr, Nico y Marian T. Adolf, «Knowledge/Power/Resistance», *Society* , 55 (2018).
Stone, Linda, «The Connected Life. From Email Apnea to Conscious Computing», *The Huffington Post* , 7 de mayo de 2012.
Stoycheff, Elizabeth, «Under Surveillance. Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Monitoring», *Journalism & Mass Communication Quarterly* , 93 (2016).
Strickland, Eliza, «How IBM Watson Overpromised and Underdelivered on AI Health Care», IEEE *Spectrum* 2 de abril de 2019.
Susskind, Jamie, *Future Politics. Living Together in a World Transformed by Tech* , Oxford, Oxford University Press, 2018.
Talisse, Robert B., «Democracy. What’s It Good for?», *The Philosophers’ Magazine* , 89 (2020).
Tandy-Connor, S., J. Guiltinan, K. Krempely, H. Laduca, P. Reineke, S. Gutierrez, P. Gray y B. Tippin Davis, «False-Positive Results Released by Direct-to-Consumer Genetic Tests Highlight the Importance of Clinical Confirmation Testing for Appropriate Patient Care», *Genetics in Medicine* , 20 (2018).
Tang, Frank, «China Names 169 People Banned from Taking Flights or Trains under Social Credit System», *South China Morning Post* , 2 de junio de 2018.
Tanner, Adam, *Our Bodies, Our Data. How Companies Make Billions Selling Our Medical Records* , Boston, Beacon Press, 2017.
Thompson, Stuart A. y Charlie Warzel, «How to Track President Trump», *The New York Times* , 20 de diciembre de 2019.
—, «Twelve Million Phones, One Dataset, Zero Privacy», *The New York Times* , 19 de diciembre de 2019.
Thomson, Amy y Jonathan Browning, «Peter Thiel’s Palantir Is Given Access to U. K. Health Data on Covid-19 Patients», *Bloomberg* , 5 de junio de 2020.
Tiku, Nitasha, «Privacy Groups Claim Online Ads Can Target Abuse Victims», *Wired* , 27 de enero de 2019.
Tondo, Lorenzo, «Scientists Say Mass Tests in Italian Town Have Halted Covid-19 There», *The Guardian* , 18 de marzo de 2020.
Trafton, Anne, «Artificial Intelligence Yields New Antibiotic», MIT News Office, 20 de febrero de 2020.
Trump, Kris-Stella, «Four and a Half Reasons Not to Worry that Cambridge Analytica Skewed the 2016 Election», *The Washington Post* , 23 de marzo de 2018.
Turton, William, «Why You Should Stop Using Telegram Right Now», *Gizmodo* , 24 de junio de 2016.
Tynan, Dan, «Facebook Says 14m Accounts Had Personal Data Stolen in Recent Breach», *The Guardian* , 12 de octubre de 2018.
«Update Report into Adtech and Real Time Bidding», Information Commissioner’s Office (ICO) (Reino Unido), 2019.
Valdés, Isabel, «La Fiscalía investiga el suicidio de una empleada de Iveco tras la difusión de un vídeo sexual», *El País* , 30 de mayo de 2019.
Valentino-Devries, Jennifer, Natasha Singer, Michael H. Keller y Aaron Krolik, «Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret», *The New York Times* , 10 de diciembre de 2018.

Véliz, Carissa, «Data, Privacy & the Individual», Center for the Governance of Change, IE University, 2020.
—, «Inteligencia artificial. ¿Progreso o retroceso?», *El País* , 14 de junio de 2019.
—, «Privacy Is a Collective Concern», *New Statesman* , 22 de octubre de 2019.
—, «Why You Might Want to Think Twice about Surrendering Online Privacy for the Sake of Convenience», *The Conversation* , 11 de enero de 2017.
—, «You've Heard of Tax Havens. After Brexit, the UK Could Become a "Data Haven"», *The Guardian* , 17 de octubre de 2020.
—, y Philipp Grunewald, «Protecting Data Privacy Is Key to a Smart Energy Future», *Nature Energy* , 3 (2018).
Victor, Daniel, «What Are Your Rights if Border Agents Want to Search Your Phone?», *The New York Times* , 14 de febrero de 2017.
Vincent, James, «iRobot's Latest Roomba Remembers Your Home's Layout and Empties Itself», *Verge* , 6 de septiembre de 2018.
Vold, Karina y Jess Whittlestone, «Privacy, Autonomy, and Personalised Targeting. Rethinking How Personal Data Is Used», en Carissa Véliz (ed.), *Data, Privacy, and the Individual* , Center for the Governance of Change, IE University, 2019.
Waddell, Kaveh, «A NASA Engineer Was Required to Unlock His Phone at the Border», *The Atlantic* , 13 de febrero de 2017.
Wakabayashi, Daisuke, «Google and the University of Chicago Are Sued over Data Sharing», *The New York Times* , 26 de junio de 2019.
Wall, Matthew, «5G: "A Cyber-Attack Could Stop the Country"», BBC News, 25 de octubre de 2018.
Wallace, Gregory, «Instead of the Boarding Pass, Bring Your Smile to the Airport», CNN, 18 de septiembre de 2018.
Wang, Echo y Carl O'Donnell, «Behind Grindr's Doomed Hookup in China, a Data Misstep and Scramble to Make Up», Reuters, 22 de mayo de 2019.
Wang, L., L. Ding, Z. Liu, L. Sun, L. Chen, R. Jia, X. Dai, J. Cao y J. Ye, «Automated Identification of Malignancy in Whole-Slide Pathological Images. Identification of Eyelid Malignant Melanoma in Gigapixel Pathological Slides Using Deep Learning», *British Journal of Ophthalmology* , 104 (2020).
Wang, Orange, «China's Social Credit System Will Not Lead to Citizens Losing Access to Public Services, Beijing Says», *South China Morning Post* , 19 de julio de 2019.
Warzel, Charlie, «Chinese Hacking Is Alarming. So Are Data Brokers», *The New York Times* , 10 de febrero de 2020.
—, y Ash Ngu, «Google's 4,000-Word Privacy Policy Is a Secret History of the Internet», *The New York Times* , 10 de julio de 2019.
Watson, Gary, «Moral Agency», en Hugh LaFollette (ed.), *The International Encyclopedia of Ethics* , Malden (Massachusetts), Wiley-Blackwell, 2013.
Weber, Max, *Economy and Society* , Berkeley, University of California Press, 1978. [Hay trad. cast.: *Economía y sociedad* , México, Fondo de Cultura Económica, 1944.]
Weinberg, Gabriel, «What if We All Just Sold Non-Creepy Advertising?», *The New York Times* , 19 de junio de 2019.
Weiss, Mark, «Digiday Research. Most Publishers Don't Benefit from Behavioral Ad Targeting», *Digiday* , 5 de junio de 2019.
Whittaker, Zack, «A Huge Database of Facebook Users' Phone Numbers Found Online», *TechCrunch* , 4 de septiembre de 2019.
«WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance», <https://www.who.int/news-room/detail/23-04-2020-whoreports-fivefold-increase-in-cyber-attacks-urges-vigilance>.
Wiener, Anna, «Taking Back Our Privacy», *The New Yorker* , 19 de octubre de 2020.
Williams, James, *Stand Out of Our Light. Freedom and Resistance in the Attention Economy* , Cambridge, Cambridge University Press, 2018.
Williams, Oscar, «Palantir's NHS Data Project "May Outlive Coronavirus Crisis"», *New Statesman* , 30 de

abril de 2020.
Wilson, James H., Paul R. Daugherty y Chase Davenport, «The Future of AI Will Be about Less Data, Not More», *Harvard Business Review* ,14 de enero de 2019.
Wilson, Jason, «Private Firms Provide Software and Information to Police, Documents Show», *The Guardian* , 15 de octubre de 2020.
Wolff, Jonathan, «The Lure of Fascism», *Aeon* , 14 de abril de 2020.
Wolfson, Sam, «Amazon's Alexa Recorded Private Conversation and Sent It to Random Contact», *The Guardian* , 24 de mayo de 2018.
—, «For My Next Trick. Dynamo's Mission to Bring Back Magic», *The Guardian* , 26 de abril de 2020.
Wong, Edward, «How China Uses LinkedIn to Recruit Spies Abroad», *The New York Times* , 27 de agosto de 2019.
Wood, Chris, «WhatsApp Photo Drug Dealer Caught by "Groundbreaking" Work», BBC News, 15 de abril de 2018.
Wu, Tim, *The Attention Merchants* , Londres, Atlantic Books, 2017. [Hay trad. cast.: *Comerciantes de atención. La lucha épica por entrar en nuestra cabeza* , Madrid, Capitán Swing, 2020.]
—, «Facebook Isn't Just Allowing Lies, It's Prioritizing Them», *The New York Times* , 4 de noviembre de 2019.
Wylie, Christopher, *Mindf*ck. Inside Cambridge Analytica's Plot to Break the World* , Londres, Profile Books, 2019.
Yadron, Danny, «Silicon Valley Tech Firms Exacerbating Income Inequality, World Bank Warns», *The Guardian* , 15 de enero de 2016.
Zetter, Kim, «How Cops Can Secretly Track Your Phone», *The Intercept* , 31 de julio de 2020.
—, «The NSA Is Targeting Users of Privacy Services, Leaked Code Shows», *Wired* , 3 de julio de 2014.
Zittrain, Jonathan, «Facebook Could Decide an Election without Anyone Ever Finding Out», *New Statesman* , 3 de junio de 2014.
—, «How to Exercise the Power You Didn't Ask for», *Harvard Business Review* , 19 de septiembre de 2018.
Zou James y Londa Schiebinger, «AI Can Be Sexist and Racist—It's Time to Make It Fair», *Nature* , 559 (2018).
Zuboff, Shoshana, *The Age of Surveillance Capitalism* , Londres, Profile Books, 2019. [Hay trad. cast.: *La era del capitalismo de la vigilancia* , Barcelona, Paidós, 2020.]

Agradecimientos

Recuperar el control de nuestros datos personales es un esfuerzo de colaboración. Este libro es el resultado de innumerables gestos altruistas de un gran número de personas, y la siguiente lista estará forzosamente incompleta. Espero que quienes no figuren en ella me perdonen y acepten también mi más sincero agradecimiento por su generosidad.

Escribí la mayor parte de este libro durante el confinamiento por la pandemia de coronavirus. Mi más profunda gratitud a todos aquellos trabajadores esenciales que arriesgaron la vida para que otros pudiéramos quedarnos en casa.

Deseo agradecer a Hertford College, al Institute for Ethics in AI, al Uehiro Centre for Practical Ethics, al Wellcome Centre for Ethics and Humanities, a Christ Church y a la Facultad de Filosofía de la Universidad de Oxford por su apoyo durante los últimos años. Gracias especialmente a Julian Savulescu por hacer del Uehiro Centre un refugio para la investigación de vanguardia en ética aplicada.

Ninguna escritora podría aspirar a tener una agente mejor que Caroline Michel. Caroline fue la primera en ver el potencial de *Privacidad es poder* cuando el libro no era aún más que una idea; sin ella, se habría quedado en eso. Gracias a todo el equipo de Peters Fraser + Dunlop. Tim Binding me animó y me ayudó a transformar un proyecto incipiente en la base de partida para todo un libro. Gracias asimismo a Laurie Robertson, Rose Brown, Rebecca Wearmouth y Lucy Barry.

Estoy agradecida a Miguel Aguilar y a todo el equipo de la editorial Debate: Roberta Gerhard y Carmen Carrión. Gracias a Albino Santos por su traducción al español.

Gracias a Nigel Warburton por pedirme que escribiera un artículo sobre privacidad para *Aeon* , que fue el que me llevó a reflexionar más a fondo sobre la relación entre la privacidad y el poder, y a *Aeon* (aeon.co) por permitirme usar ese texto como base del capítulo 3 de este libro.

Desde que empecé a investigar el tema de la privacidad, me he beneficiado de conversaciones inspiradoras con numerosos y brillantes mentores y colegas. Mis directores de tesis doctoral, Roger Crisp y Cécile Fabre, han tenido un papel crucial en la revisión y perfeccionamiento de mis ideas sobre la privacidad. También han sido interlocutores importantes para mí Anabelle Lever, Antonio Diéguez, Carina Prunkl, Ellen Judson, Evan Selinger, Gemma Galdon Clavell,

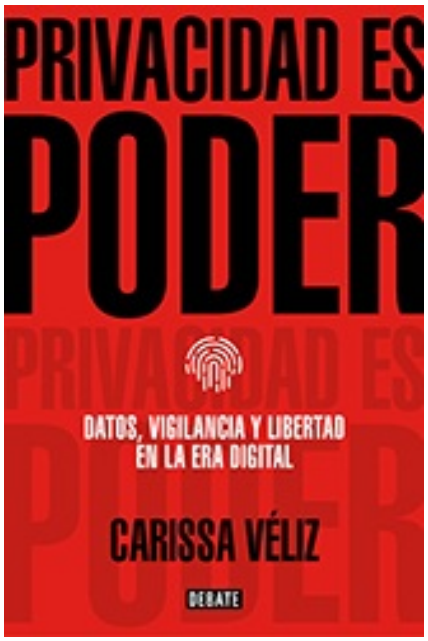
Gina Neff, Gopal Sreenivasan, Katrien Devolder, James Williams, Jeff McMahan, Julia Powles, Julian Savulescu, Kevin Macnish, Lindsay Judson, Marjolein Lanzing, Peter Millican y todos los conferenciantes del Seminario sobre Ética en IA de la Universidad de Oxford, Tom Douglas, Václav Janecˇek e Yves-Alexandre de Montjoye, entre otros muchos.

Las siguientes personas fueron muy amables por leer partes del libro, o incluso el manuscrito completo, y lo mejoraron con sus comentarios. Gracias a Bent Flyvbjerg, Javier de la Cueva, Ian Preston, Jo Wolff, Jorge Volpi, Diego Rubio, Yves-Alexandre de Montjoye, Mark Lewis, Marta Dunphy-Moriel y Peter Millican por ayudarme a detectar errores. Soy, por supuesto, la única responsable de todos los fallos y descuidos que, aun así, hayan podido quedar.

Agradezco a todos mis amigos y seres queridos por haberme apoyado en todo momento. Muchas gracias a Aitor Blanco, Alberto Giubilini, Areti Theofilopoulou, Daniela Torres, David Ewert, Diego Rubio, Hannah Maslen, Javier de la Cueva, Josh Shepherd, Kyo Ikeda, Luciano Espinosa, María Teresa López de la Vieja, Marina LópezSolà, Rafo Mejía, Ricardo Parellada, Rosana Triviño, Stella Villarmea, Susan Greenfield y Txetxu Ausín, entre otros muchos que me han ayudado a lo largo de estos años. Un agradecimiento especialmente afectuoso a Marisol Gandía, Sole y Maite Vidal, Silvia Gandía, y al resto de mi familia valenciana.

No hay palabras para expresar mi gratitud a Héctor, María, Iván y Julián: mis salvavidas y consejeros, y las mejores personas que conozco. Gracias de todo corazón a Ale y Alexis, y a las pequeñas. Y, por último, gracias a Bent Flyvbjerg por animarme a escribir, por leer a mi lado, por escribir algo más que palabras conmigo. Siempre estaré agradecida de que, a pesar de la oscuridad y la angustia que trajo consigo la pandemia, fui una de las personas afortunadas para las que el confinamiento tuvo un lado positivo: tuve la suerte de estar encerrada en casa con la persona adecuada, escribiendo este libro.

Seleccionado por *The Economist* como uno de los libros del año.
La guía definitiva para afrontar uno de los problemas más acuciantes de nuestro tiempo: la pérdida de la privacidad.



Nos vigilan. Saben que estás leyendo estas palabras. Gobiernos y cientos de empresas nos espían: a ti y a todos tus conocidos. A todas horas, todos los días. Rastrean y registran todo lo que pueden: nuestra ubicación, nuestras comunicaciones, nuestras búsquedas en internet, nuestra información biométrica, nuestras relaciones sociales, nuestras compras, nuestros problemas médicos y mucho más

Quieren saber quiénes somos, qué pensamos, dónde nos duele. Quieren predecir nuestro comportamiento e influir en él. Tienen demasiado poder. Su poder proviene de nosotros, de ti, de tus datos. Recuperar la privacidad es la única manera de que podamos asumir de nuevo el mando de nuestras vidas y de nuestras sociedades. La privacidad es tan colectiva como personal, y es hora de retomar el control.

Privacidad es poder es el primer libro que propone el fin de la economía de los datos. Carissa Véliz explica cómo nuestros datos personales están cediendo demasiado poder a las grandes empresas tecnológicas y a los gobiernos, por qué esto es importante y qué podemos hacer al respecto.

Carissa Véliz es profesora asociada de la Facultad de Filosofía y del Instituto de Ética de Inteligencia Artificial, así como miembro del Hertford College de la Universidad de Oxford. Véliz ha publicado artículos en *The Guardian, The New York Times, New Statesman y The Independent* . Su trabajo académico se ha publicado en *The Harvard Business Review, Nature Electronics, Nature Energy y The American Journal of Bioethics* , entre otras revistas. Es la editora del *Oxford Handbook of Digital Ethic*



Título original: *Privacy Is Power. Why and How You Should Take Back Control of Your Data*

Edición en formato digital: septiembre de 2021

© 2020, Carissa Véliz
© 2021, Penguin Random House Grupo Editorial, S.A.U.
Travessera de Gràcia, 47-49. 08021 Barcelona
© 2021, Albino Santos Mosquera, por la traducción. Traducción revisada por la autora

Diseño de portada: Adaptación del diseño original de Richard Ogle/TW.
Penguin Random House Grupo Editorial
Imagen de portada: © Shutterstock

Penguin Random House Grupo Editorial apoya la protección del *copyright* . El *copyright* estimula la creatividad, defiende la diversidad en el ámbito de las ideas y el conocimiento, promueve la libre expresión y favorece una cultura viva. Gracias por comprar una edición autorizada de este libro y por respetar las leyes del *copyright* al no reproducir ni distribuir ninguna parte de esta obra por ningún medio sin permiso. Al hacerlo está respaldando a los autores y permitiendo que PRHGE continúe publicando libros para todos los lectores. Diríjase a CEDRO (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita reproducir algún fragmento de esta obra.

ISBN: 978-84-1805-669-7

Composición digital: Newcomlab S.L.L.

Facebook: PenguinEbooks Facebook: debatelibros Twitter: @debatelibros Instagram: @debatelibros
YouTube: penguinlibros Spotify: PenguinLibros

Introducción

[1] A lo largo del libro, uso los conceptos «economía de los datos», «economía de la vigilancia», «capitalismo de la vigilancia» y «sociedad de la vigilancia» de forma casi indistinta. En teoría, podría haber una economía de los datos que excluyera los que fueran «personales». Se podría comerciar con información impersonal. Sin embargo, en el momento de escribir estas líneas, cuando hablamos de la «economía de los datos», solemos referirnos al comercio de información relativa a las personas, y por eso utilizo «economía de los datos» como una forma abreviada de aludir a la «economía de los datos personales».

[2] En la primera película de la saga *Matrix* , Trinity y Morfeo también tuvieron que llegar hasta Neo a través de Matrix para sacarlo de esta.

[3] Brittany Kaiser, *Targeted. My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy* , Londres, HarperCollins, 2019, p. 81. [Hay trad. cast.: *La dictadura de los datos. La verdadera historia desde dentro de Cambridge Analytica y de cómo el Big Data, Trump y Facebook rompieron la democracia y cómo puede volver a pasar* , Barcelona, HarperCollins, 2019.]

1. Buitres de datos

[1] Sobre la «automonitorización», véase Gina Neffy Dawn Nafus, *Self-Tracking* , Cambridge (Massachusetts), MIT Press, 2016.

[2] Aliya Ram y Emma Boyde, «People Love Fitness Trackers, but Should Employers Give Them Out?», *Financial Times* , 16 de abril de 2018.

[3] Ifeoma Ajunwa, Kate Crawford y Jason Schultz, «Limitless Worker Surveillance», *California Law Review* , 105 (2017), pp. 766-767.

[4] Sam Biddle, «For Owners of Amazon’s Ring Security Cameras, Strangers May Have Been Watching Too», *The Intercept* , 10 de enero de 2019.

[5] Geoffrey Fowler, «The Doorbells Have Eyes. The Privacy Battle Brewing over Home Security Cameras», *The Washington Post* , 31 de enero de 2019.

[6] Alex Hern, «Smart Electricity Meters Can Be Dangerously Insecure, Warns Expert», *The Guardian* , 29 de diciembre de 2016.

[7] Carissa Véliz y Philipp Grunewald, «Protecting Data Privacy Is Key to a Smart Energy Future», *Nature Energy* , 3 (2018).

[8] L. Stanokvic, V. Stanokvic, J. Liao y C. Wilson, «Measuring the Energy Intensity of Domestic Activities from Smart Meter Data», *Applied Energy* , 183 (2016).

[9] Alex Hern, «UK Homes Vulnerable to “Staggering” Level of Corporate Surveillance», *The Guardian* , 1 de junio de 2018.

[10] <https://www.samsung.com/hk_en/info/privacy/smarttv>, consultada el 7 de mayo de 2020.

[11] Nicole Nguyen, «If You Have a Smart TV, Take a Closer Look at Your Privacy Settings», CNBC , 9 de marzo de 2017.

[12] Matt Burgess, «More than 1,000 UK Schools Found to Be Monitoring Children with Surveillance Software», *Wired* , 8 de noviembre de 2016.

[13] Lily Hay Newman, «How to Block the Ultrasonic Signals You Didn’t Know Were Tracking You», *Wired* , 3 de noviembre de 2016.

[14] Una versión parecida de esa explicación fue la que dio un portavoz de Amazon cuando Alexa grabó la conversación privada de una persona y la envió a uno de sus contactos. Sam Wolfson, «Amazon’s Alexa Recorded Private Conversation and Sent It to Random Contact», *The Guardian* , 24 de mayo de 2018.

[15] Daniel J. Dubois, Roman Kolcun, Anna Maria Mandalari, Muhammad Talha Paracha, David

Choffnes y Hamed Haddadi, «When Speakers Are All Ears», *Proceedings on 20th Privacy Enhancing Technologies Symposium* , 2020.

[16] S. Wolfson, «Amazon's Alexa Recorded Private Conversation...».

[17] Michael Baxter, «Do Connected Cars Pose a Privacy Threat?», *GDPR . Report* , 1 de agosto de 2018.

[18] Erin Biba, «How Connected Car Tech Is Eroding Personal Privacy», BBC News, 9 de agosto de 2016; John R. Quain, «Cars Suck Up Data about You. Where Does It All Go?», *The New York Times* , 27 de julio de 2017.

[19] Bruce Schneier, *Data and Goliath* , Londres, Nueva York, W. W. Norton & Company, 2016, p. 68. IMSI son las siglas en inglés de «identidad internacional de abonado móvil».

[20] <https://www.aclu.org/issues/privacy-technology/surveillancetechnologies/stingray-tracking-devices-whos-got-them>, consultado el 15 de octubre de 2020.

[21] Kim Zetter, «How Cops Can Secretly Track Your Phone», *The Intercept* , 31 de julio de 2020.

[22] K. Zetter, «How Cops Can Secretly Track Your Phone».

[23] Ben Bryant, «VICE News Investigation Finds Signs of Secret Phone Surveillance Across London», *Vice* , 14 de enero de 2016.

[24] Quedarse sin aliento ante lo que se ve en la pantalla o en el correo electrónico tiene un nombre. Se llama «apnea del correo electrónico» o «apnea de la pantalla». Linda Stone, «The Connected Life. From Email Apnea to Conscious Computing», *The Huffington Post* , 7 de mayo de 2012.

[25] Steven Englehardt, Jeffrey Han y Arvind Narayanan, «I Never Signed Up For This! Privacy Implications of Email Tracking», *Proceedings on Privacy Enhancing Technologies* , 1 (2018); Brian Merchant, «How Email Open Tracking Quietly Took Over the Web», *Wired* , 11 de diciembre de 2017.

[26] Radhika Sanghani, «Your Boss Can Read Your Personal Emails. Here's What You Need to Know», *The Telegraph* , 14 de enero de 2016.

[27] Kristen V. Brown, «What DNA Testing Companies' Terrifying Privacy Policies Actually Mean», *Gizmodo* , 18 de octubre de 2017.

[28] Bradley Malin y Latanya Sweeney, «Determining the Identifiability of DNA Database Entries», *Proceedings, Journal of the American Medical Informatics Association* , febrero de 2000.

[29] S. Tandy-Connor, J. Guiltinan, K. Krempely, H. LaDuca, P. Reineke, S. Gutierrez, P. Gray y B. Tippin Davis, «False-Positive Results Released by Direct-to-Consumer Genetic Tests Highlight the Importance of Clinical Confirmation Testing for Appropriate Patient Care», *Genetics in Medicine* , 20 (2018).

[30] Richie Koch, «Using Zoom? Here Are the Privacy Issues You Need to Be Aware Of», *ProtonMail* , 20 de marzo de 2020.

[31] Cuando las comunicaciones están cifradas de extremo a extremo, las empresas no pueden acceder a su contenido. Sin embargo, Zoom podía acceder al vídeo y el audio de las reuniones, aun cuando su aplicación de escritorio decía que estaba usando un cifrado de extremo a extremo. Micah Lee y Yael Grauer, «Zoom Meetings Aren't End-to-End Encrypted, despite Misleading Marketing», *The Intercept* , 31 de marzo de 2020. Unos meses más tarde, cuando la noticia se hizo pública, Zoom anunció que iba a excluir de ese sistema de cifrado todas las llamadas gratuitas. Tras la reacción adversa que esto suscitó en los usuarios, preocupados por su privacidad, prometió que todos los usuarios estarían cubiertos por el cifrado de extremo a extremo. Kari Paul, «Zoom to Exclude Free Calls from End-to-End Encryption to Allow FBI Cooperation», *The Guardian* , 4 de junio de 2020; Kari Paul, «Zoom Will Provide End-to-End Encryption to All Users after Privacy Backlash», *The Guardian* , 17 de junio de 2020.

[32] Michael Grothaus, «Forget the New iPhones. Apple's Best Product Is Now Privacy», *Fast Company* , 13 de septiembre de 2018.

[33] Casey Johnston, «Facebook Is Tracking Your "Self-Censorship"», *Wired* , 17 de diciembre de 2013.

[34] Kashmir Hill, «How Facebook Outs Sex Workers», *Gizmodo* , 10 de noviembre de 2017.

[35] Kashmir Hill, «Facebook Recommended that This Psychiatrist's Patients Friend Each Other», Splinter News, 29 de agosto de 2016.

[36] Kashmir Hill, «"People You May Know": A Controversial Facebook Feature's 10-Year History»,

Gizmodo , 8 de agosto de 2018.

[37] «Facebook Fined £500,000 for Cambridge Analytica Scandal», BBC News, 25 de octubre de 2018.

[38] Dan Tynan, «Facebook Says 14m Accounts Had Personal Data Stolen in Recent Breach», *The Guardian* , 12 de octubre de 2018.

[39] Gabriel J. X. Dance, Michael LaForgia y Nicholas Confessore, «As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants», *The New York Times* , 18 de diciembre de 2018.

[40] Kashmir Hill, «Facebook Was Fully Aware that Tracking Who People Call and Text Is Creepy but Did It Anyway», *Gizmodo* , 12 de mayo de 2018.

[41] Natasha Singer, «Facebook's Push for Facial Recognition Prompts Privacy Alarms», *The New York Times* , 9 de julio de 2018.

[42] Alex Hern, «Facebook Faces Backlash over Users' Safety Phone Numbers», *The Guardian* , 4 de marzo de 2019.

[43] Zack Whittaker, «A Huge Database of Facebook Users' Phone Numbers Found Online», *TechCrunch* , 4 de septiembre de 2019.

[44] Associated Press, «Facebook Data Leak: Details From 533 Million Users Found on Website for Hackers», *The Guardian* , 5 de abril de 2021.

[45] David Gilbert, «Facebook Says It's Your Fault That Hackers Got Half a Billion User Phone Numbers», *Vice* , 7 de abril de 2021.

[46] Véase una lista de los desastres cometidos por Facebook en materia de privacidad entre 2006 y 2018 en Natasha Lomas, «A Brief History of Facebook's Privacy Hostility ahead of Zuckerberg's Testimony», *TechCrunch* , 10 de abril de 2018.

[47] Len Sherman, «Zuckerberg's Broken Promises Show Facebook Is Not Your Friend», *Forbes* ,23 de mayo de 2018. «Pese a las reiteradas promesas hechas a sus miles de millones de usuarios en todo el mundo de que estos podrían controlar cómo se comparte su información, Facebook cercenó las opciones de los consumidores», dijo el presidente de la Comisión Federal de Comercio (FTC), Joe Simons. Comunicado de prensa de la FTC , «FTC Settlement Imposes Historic Penalty, and Significant Requirements to Boost Accountability and Transparency», 24 de julio de 2019.

[48] Allen St. John, «How Facebook Tracks You, Even When You're Not on Facebook», *Consumer Reports* , 11 de abril de 2018.

[49] Comisión de Asuntos Digitales, Cultura, Medios y Deporte, «Disinformation and "Fake News": Final Report», Cámara de los Comunes, 2019.

[50] Brian Fung, «How Stores Use Your Phone's WiFi to Track Your Shopping Habits», *The Washington Post* , 19 de octubre de 2013.

[51] Stephanie Clifford y Quentin Hardy, «Attention, Shoppers. Store Is Tracking Your Cell», *The New York Times* , 14 de julio de 2013.

[52] Chris Frey, «Revealed. How Facial Recognition Has Invaded Shops—and Your Privacy», *The Guardian* , 3 de marzo de 2016.

[53] Kashmir Hill y Aaron Krolik, «How Photos of Your Kids Are Powering Surveillance Technology», *The New York Times* , 11 de octubre de 2019.

[54] Yael Grauer, «What Are "Data Brokers", and Why Are They Scooping Up Information about You?», *Motherboard* , 27 de mayo de 2018.

[55] Adam Tanner, *Our Bodies, Our Data. How Companies Make Billions Selling Our Medical Records* , Boston, Beacon Press, 2017, pp. 78, 95 y 147148.

[56] Julia Powles y Hal Hodson, «Google DeepMind and Healthcare in an Age of Algorithms», *Health and Technology* , 7 (2017).

[57] Daisuke Wakabayashi, «Google and the University of Chicago Are Sued over Data Sharing», *The New York Times* , 26 de junio de 2019.

[58] Dan Munro, «Data Breaches in Healthcare Totaled over 112 Million Records in 2015», *Forbes* , 31 de diciembre de 2015.

[59] Alex Hern, «Hackers Publish Private Photos from Cosmetic Surgery Clinic», *The Guardian* , 31 de

mayo de 2017.
[60] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller y Aaron Krolik, «Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret», *The New York Times* , 10 de diciembre de 2018.
[61] Nick Statt, «How AT&T's Plan to Become the New Facebook Could Be a Privacy Nightmare», *Verge* , 16 de julio de 2018.
[62] Si la privacidad fuera una prioridad, las operadoras móviles podrían diseñar un sistema para no saber automáticamente la ubicación de sus clientes. Manuel G. Pascual, «En busca de un móvil que no nos rastree», *El País* , 1 de marzo de 2021.
[63] Joseph Cox, «I Gave a Bounty Hunter $300. Then He Located Our Phone», *Motherboard* , 8 de enero de 2019.
[64] Olivia Solon, «"Data Is a Fingerprint": Why You Aren't as Anonymous as You Think Online», *The Guardian* , 13 de julio de 2018.
[65] Yves-Alexandre de Montjoye, C. A. Hidalgo, M. Verleysen y V. D. Blondel, «Unique in the Crowd. The Privacy Bounds of Human Mobility», *Scientific Reports* , 3 (2013).
[66] Yves-Alexandre de Montjoye, L. Radaelli, V. K. Singh y A. S. Pentland, «Identity and Privacy. Unique in the Shopping Mall. On the Reidentifiability of Credit Card Metadata», *Science* , 347 (2015).
[67] Ryan Singel, «Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims», *Wired* , 17 de diciembre de 2009.
[68] Aliya Ram y Madhumita Murgia, «Data Brokers. Regulators Try To Rein In the "Privacy Deathstars"», *Financial Times* , 8 de enero de 2019.
[69] Natasha Singer, «Data Broker Is Charged with Selling Consumers' Financial Details to "Fraudsters"», *The New York Times* , 23 de diciembre de 2014.
[70] Melanie Hicken, «Data Brokers Selling Lists of Rape Victims, AIDS Patients», CNN , 19 de diciembre de 2013.
[71] Nitasha Tiku, «Privacy Groups Claim Online Ads Can Target Abuse Victims», *Wired* , 27 de enero de 2019.
[72] Nicole Kobie, «Heathrow's Facial Recognition Tech Could Make Airports More Bearable», *Wired* , 18 de octubre de 2018; Gregory Wallace, «Instead of the Boarding Pass, Bring Your Smile to the Airport», CNN , 18 de septiembre de 2018.
[73] Davey Alba, «The US Government Will Be Scanning Your Face at 20 Top Airports, Documents Show», BuzzFeed, 11 de marzo de 2019.
[74] Kaveh Waddell, «A NASA Engineer Was Required to Unlock His Phone at the Border», *The Atlantic* , 13 de febrero de 2017.
[75] Daniel Victor, «What Are Your Rights if Border Agents Want to Search Your Phone?», *The New York Times* , 14 de febrero de 2017.
[76] Gemma Galdon Clavell, «Protect Rights at Automated Borders», *Nature* , 543 (2017).
[77] Olivia Solon, «"Surveillance Society". Has Technology at the US-Mexico Border Gone Too Far?», *The Guardian* , 13 de junio de 2018.
[78] Douglas Heaven, «An AI Lie Detector Will Interrogate Travellers at some EU Borders», *New Scientist* , 31 de octubre de 2018.
[79] Dylan Curran, «Are You Ready? Here Is All the Data Facebook and Google Have on You», *The Guardian* , 30 de marzo de 2018.
[80] John Naughton, «More Choice on Privacy Just Means More Chances to Do What's Best for Big Tech», *The Guardian* , 8 de julio de 2018.
[81] Alex Hern, «Privacy Policies of Tech Giants "Still Not GDPR -Compliant"», *The Guardian* , 5 de julio de 2018.
[82] Logan Koepke, «"We Can Change These Terms at Anytime". The Detritus of Terms of Service Agreements», *Medium* , 18 de enero de 2015.
[83] J. Naughton, «More Choice on Privacy...».

[84] Arwa Mahdawi, «Spotify Can Tell if You’re Sad. Here’s Why That Should Scare You», *The Guardian* , 16 de septiembre de 2018.

[85] Alfred Ng, «With Smart Sneakers, Privacy Risks Take a Great Leap», CNET , 13 de febrero de 2019.

[86] Christopher Mims, «Here Comes “Smart Dust”, the Tiny Computers That Pull Power from the Air», *The Wall Street Journal* , 8 de noviembre de 2018.

2. ¿Cómo hemos llegado a esto?

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism* , Londres, Profile Books, 2019, cap. 3. [Hay trad. cast.: *La era del capitalismo de la vigilancia* , Barcelona, Paidós, 2020.]

[2] Samuel Gibbs y Alex Hern, «Google at 20. How Two “Obnoxious” Students Changed the Internet», *The Guardian* , 24 de septiembre de 2018.

[3] John Battelle, «The Birth of Google», *Wired* , 1 de agosto de 2005.

[4] S. Gibbs y A. Hern, «Google at 20. How Two “Obnoxious” Students Changed the Internet»...

[5] Steven Levy, *In the Plex. How Google Thinks, Works, and Shapes Our Lives* , Nueva York, Simon & Schuster, 2011, pp. 77-78.

[6] Informe anual de Google a la Comisión del Mercado de Valores de Estados Unidos correspondiente al ejercicio de 2004, <https://www.sec. gov/Archives/edgar/data/1288776/000119312505065298/d10k.htm>.

[7] Sergey Brin y Lawrence Page, «The Anatomy of a Large-Scale Hypertextual Web Search Engine», *Computer Networks and ISDN Systems* , 30 (1998).

[8] S. Levy, *In the Plex* ..., p. 82.

[9] S. Gibbs y A. Hern, «Google at 20. How Two “Obnoxious” Students Changed the Internet»..., pp. 89-90.

[10] Informe anual de Alphabet Inc. a la Comisión del Mercado de Valores de Estados Unidos correspondiente al ejercicio de 2019, <https://abc. xyz/investor/static/pdf/20200204_alphabet_10K.pdf?cache=cdd6dbf>.

[11] Richard Graham, «Google and Advertising. Digital Capitalism in the Context of Post-Fordism, the Reification of Language, and the Rise of Fake News», *Palgrave Communications* , 3 (2017), p. 2.

[12] Jennifer Lee, «Postcards From Planet Google», *The New York Times* , 28 de noviembre de 2002.

[13] J. Lee, «Postcards From Planet Google»...

[14] Krishna Bharat, Stephen Lawrence y Merhan Sahami, «Generating User Information for Use in Targeted Advertising», 2003.

[15] La última jugada de Google para seguir dominando la economía de la vigilancia es el plan de bloquear *cookies* para terceros usando nuevas tecnologías (FLOC) para «minar» los mismos datos que antes: Manuel G. Pascal, «El fin de las *cookies* de terceros: ¿hacia una nueva era del negocio digital?», *El País* , 18 de marzo de 2021. Bennett Cyphers, «Google’s FLOC Is a Terrible Idea», *Electronic Frontier Foundation* , 3 de marzo de 2002.

[16] S. Levy, *In the Plex* ..., pp. 330-336.

[17] S. Zuboff, *The Age of Surveillance Capitalism* ..., pp. 87-92.

[18] S. Levy, *In the Plex* ..., p. 68.

[19] Douglas Edwards, *I’m Feeling Lucky. The Confessions of Google Employee Number 59* , Boston y Nueva York, Houghton Mifflin Harcourt, 2011, p. 340.

[20] S. Zuboff, *The Age of Surveillance Capitalism* ..., p. 89.

[21] Louise Matsakis, «The WIRED Guide to Your Personal Data (and Who Is Using It)», *Wired* , 15 de febrero de 2019.

[22] «Privacy Online. Fair Information Practices in the Electronic Marketplace. A Report to Congress», Federal Trade Commission, 2000.

[23] S. Zuboff, *The Age of Surveillance Capitalism* ..., pp. 112-121.

[24] Bruce Schneier, *Click Here to Kill Everybody. Security and Survival in a Hyper-Connected World* , Nueva York, W. W. Norton & Company, 2018, p. 65. [Hay trad. cast.:*Haz clic para matarlos a todos. Un manual de supervivencia* , Barcelona, Temas de Hoy, 2019.]

[25] Babu Kurra, «How 9/11 Completely Changed Surveillance in U. S.», *Wired* , 11 de septiembre de 2011.

[26] Edward Snowden, *Permanent Record* , Londres, Macmillan, 2019. [Hay trad. cast.: *Vigilancia permanente* , Barcelona, Planeta, 2019.]

[27] Para saber más sobre vigilancia estatal en Estados Unidos y sobre las revelaciones de Edward Snowden, recomiendo leer el detallado relato que de todo ello hace Barton Gellman en su libro *Dark Mirror* , así como la autobiografía del propio Snowden. Barton Gellman, *Dark Mirror* , Londres, Bodley Head, 2020.

[28] E. Snowden, *Permanent Record* ..., pp. 223-224.

[29] E. Snowden, *Permanent Record* ..., pp. 278-279.

[30] E. Snowden, *Permanent Record* ..., p. 163.

[31] E. Snowden, *Permanent Record* ..., p. 225.

[32] E. Snowden, *Permanent Record* ..., pp. 167-168.

[33] Michael Isikoff, «NSA Program Stopped No Terror Attacks, Says White House Panel Member», NBC News, 20 de diciembre de 2013.

[34] Charlie Savage, «Declassified Report Shows Doubts about Value of N. S. A.'s Warrantless Spying», *The New York Times* , 24 de abril de 2015.

[35] Charlie Savage, *Power Wars. Inside Obama's Post-9/11 Presidency* , Nueva York, Little, Brown & Company, 2015, pp. 162-223.

[36] Inspector general de la NSA , «Report on the President's Surveillance Program», NSA , 2009, p. 637.

[37] Para entender mejor por qué la vigilancia masiva no es el enfoque correcto para prevenir el terrorismo, véase B. Schneier, *Data and Goliath* ..., pp. 135-139.

[38] James Glanz y Andrew W. Lehren, «NSA Spied on Allies, Aid Groups and Businesses», *The New York Times* , 21 de diciembre de 2013.

[39] Julia Angwin, JeffLarson, Charlie Savage, James Risen, Henrik Moltke y Laura Poitras, «NSA Spying Relies on AT&T's "Extreme Willingness to Help"», *ProPublica* , 15 de agosto de 2015.

[40] Jebediah Purdy, «The Anti-Democratic Worldview of Steve Bannon and Peter Thiel», *Politico* , 30 de noviembre de 2016.

[41] Sam Biddle, «How Peter Thiel's Palantir Helped the NSA Spy on the Whole World», *The Intercept* , 22 de febrero de 2017.

[42] B. Schneier, *Click Here to Kill Everybody* ..., p. 65.

[43] Sam Levin, «Tech Firms Make Millions from Trump's Anti-Immigrant Agenda, Report Finds», *The Guardian* , 23 de octubre de 2018.

[44] Amanda Holpuch, «Trump's Separation of Families Constitutes Torture, Doctors Find», *The Guardian* , 25 de febrero de 2020.

[45] Jason Wilson, «Private Firms Provide Software and Information to Police, Documents Show», *The Guardian* , 15 de octubre de 2020.

[46] Alfred Ng, «Google Is Giving Data to Police Based on Search Keywords, Court Docs Show», CNET , 8 de octubre de 2020.

[47] «The Government Uses "Near Perfect Surveillance" Data on Americans», editorial, *The New York Times* , 7 de febrero de 2020. Joseph Cox, «CBP Refuses to Tell Congress How It Is Tracking Americans without a Warrant», *Vice* , 23 de octubre de 2020.

[48] Toby Helm, «Patient Data From GP Surgeries Sold to US Companies», *The Observer* , 7 de diciembre de 2019.

[49] Juliette Kayyem, «Never Say "Never Again"», *Foreign Policy* , 11 de septiembre de 2012.

[50] Bobbie Johnson, «Privacy No Longer a Social Norm, Says Facebook Founder», *The Guardian* , 11 de enero de 2010.

[51] Alyson Shontell, «Mark Zuckerberg Just Spent More than $30 Million Buying 4 Neighboring Houses for Privacy», *Business Insider* , 11 de octubre de 2013.

[52] Bobbie Johnson, «Facebook Privacy Change Angers Campaigners», *The Guardian* , 10 de diciembre de 2009.

[53] Doy las gracias a Judith Curthoys por este ejemplo. Según me contó Ellen Judson, uno de los directores de un *college* de Cambridge también pudo tener allí un perro que las normas prohibían porque se catalogó como un «gato muy grande», <https://www.bbc.co.uk/news/uk-englandcambridgeshire-28966001>.

[54] Harry Cockburn, «The UK'S Strangest Laws That Are Still Enforced», *The Independent* , 8 de septiembre de 2016.

[55] Nick Statt, «Facebook CEO Mark Zuckerberg Says the "Future Is Private"», *Verge* , 30 de abril de 2019.

[56] Sam Biddle, «In Court, Facebook Blames Users for Destroying Their Own Right to Privacy», *The Intercept* , 14 de junio de 2014.

[57] Roxanne Bamford, Benedict Macon-Cooney, Hermione Dace y Chris Yiu, «A Price Worth Paying. Tech, Privacy and the Fight against Covid-19», Tony Blair Institute for Global Change, 2020.

[58] Barrington Moore, *Privacy. Studies in Social and Cultural History* , Armonk (Nueva York), M. E. Sharpe, 1984.

[*] No todas las empresas se mostraron igual de contentas de colaborar con la vigilancia masiva, pero todas tuvieron que obedecer.

[**] Peter Thiel es un multimillonario emprendedor e inversor de capital riesgo famoso por sus opiniones antiliberales. Ha escrito que no cree «que la libertad y la democracia sean compatible». Dado que considera que la libertad es «una condición previa para el bien supremo», la implicación parece ser que ya no es partidario de la democracia.

3. Privacidad es poder

[1] Tim Wu, *The Attention Merchants* , Londres, Atlantic Books, 2017 [hay trad. cast.: *Comerciantes de atención. La lucha épica por entrar en nuestra cabeza* , Madrid, Capitán Swing, 2020];James Williams, *Stand Out of Our Light. Freedom and Resistance in the Attention Economy* , Cambridge, Cambridge University Press, 2018.

[2] Alex Hern, «Netflix's Biggest Competitor? Sleep», *The Guardian* , 18 de abril de 2017.

[3] Aunque en este libro uso la palabra «jáqueres» en su acepción más común para referirme a las personas que se introducen sin permiso en los sistemas de seguridad, el término más exacto sería «*crackers* ». Los *crackers* son los jáqueres maliciosos. Véase Richard Stallman, «On Hacking», <https://stallman.org/articles/on-hacking.html>.

[4] Oliver Ralph, «Insurance and the Big Data Technology Revolution», *Financial Times* , 24 de febrero de 2017.

[5] Dave Smith y Phil Chamberlain, «On the Blacklist. How Did the UK'S Top Building Firms Get Secret Information on Their Workers», *The Guardian* , 27 de febrero de 2015.

[6] Rupert Jones, «Identity Fraud Reaching Epidemic Levels, New Figures Show», *The Guardian* , 23 de agosto de 2017.

[7] Kaleigh Rogers, «Let's Talk about Mark Zuckerberg's Claim that Facebook "Doesn't Sell Data"», *Motherboard* , 11 de abril de 2019.

[8] Charlie Warzel y Ash Ngu, «Google's 4,000-Word Privacy Policy Is a Secret History of the Internet», *The New York Times* , 10 de julio de 2019.

[9] Rainer Forst, «Noumenal Power», *The Journal of Political Philosophy* , 23 (2015).

[10] Max Weber, *Economy and Society* , Berkeley, University of California Press, 1978, p. 53. [Hay trad. cast.: *Economía y sociedad* , México, Fondo de Cultura Económica, 1944, p. 43.]

[11] Bertrand Russell, *Power. A New Social Analysis* , Londres, Routledge, 2004, p. 4. [Hay trad. cast.: *El poder. Un nuevo análisis social* , Barcelona, RBA , 2010.]

[12] Michel Foucault, *Discipline and Punish* , Londres, Penguin, 1977 [hay trad. cast.: *Vigilar y castigar* , Ciudad de México, Siglo XXI , 1976]; Nico Stehr y Marian T. Adolf, «Knowledge/Power/Resistance», *Society* , 55 (2018).

[13] Hubert Dreyfus y Paul Rabinow, *Michel Foucault. Beyond Structuralism and Hermeneutics* , Chicago, The University of Chicago Press, 1982, p. 212. [Hay trad. cast.:*Michel Foucault. Más allá del estructuralismo y la hermenéutica* , Buenos Aires, Nueva Visión, 2001.]

[14] Steven Lukes, *Power. A Radical View* , Londres, Red Globe Press, 2005. [Hay trad. cast.: *El poder. Un enfoque radical* , Madrid, Siglo XXI, 1985.]

[15] Simon Parkin, «Has Dopamine Got Us Hooked on Tech?», *The Guardian* , 4 de marzo de 2018.

[16] <https://www.britannica.com/topic/Stasi>.

[17] Andrea Peterson, «Snowden Filmmaker Laura Poitras:“Facebook Is a Gift to Intelligence Agencies”», *The Washington Post* , 23 de octubre de 2014.

[18] Robert Booth, Sandra Laville y Shiv Malik, «Royal Wedding. Police Criticised for Pre-Emptive Strikes against Protestors», *The Guardian* , 29 de abril de 2011.

[19] Tae Kim, «Warren Buffett Believes This Is “the Most Important Thing” to Find in a Business», CNBC , 7 de mayo de 2018.

[20] Associated Press, «Google Records Your Location Even When You Tell It Not to», *The Guardian* , 13 de agosto de 2018.

[21] Frank Tang, «China Names 169 People Banned from Taking Flights or Trains under Social Credit System», *South China Morning Post* , 2 de junio de 2018.

[22] Simina Mistreanu, «Life inside China’s Social Credit Laboratory», *Foreign Policy* , 3 de abril de 2018.

[23] Orange Wang, «China’s Social Credit System Will Not Lead to Citizens Losing Access to Public Services, Beijing Says», *South China Morning Post* , 19 de julio de 2019.

[24] Nectar Gan, «China Is Installing Surveillance Cameras Outside People’s Front Doors—and Sometimes Inside Their Homes», *CNN Business* , 28 de abril de 2020.

[25] En su artículo, Hill menciona una lista de otras empresas que puntúan a los consumidores y cómo contactar con ellas para pedirles nuestros datos. Kashmir Hill, «I Got Access to My Secret Consumer Score. Now You Can Get Yours, Too», *The New York Times* , 4 de noviembre de 2019.

[26] Un excelente libro sobre el tecnoautoritarismo en China es *We Have Been Harmonised* , por Kai Strittmatter (Old Street Publishing, 2019).

[27] E. Snowden, *Permanent Record* ..., pp. 196-197.

[28] Jamie Susskind, *Future Politics. Living Together in a World Transformed by Tech* , Oxford University Press, 2018, pp. 103-107.

[29] J. Susskind, *Future Politics* ..., p. 172.

[30] Esta idea de que la manipulación hace que la víctima sea cómplice de su propia victimización la he tomado del filósofo Robert Noggle. Workshop on Behavioural Prediction and Influence, «The Moral Status of “Other Behavioral Influences”», Universidad de Oxford, 27 de septiembre de 2019.

[31] Richard Esguerra, «Google CEO Eric Schmidt Dismisses the Importance of Privacy», Electronic Frontier Foundation, 10 de diciembre de 2009.

[32] S. Levy, *In the Plex* ..., p. 175.

[33] Existen motivos para defender el argumento de que se nos debería permitir ocultar las transgresiones menores (como hace, por ejemplo, Cressida Gaukroger, «Privacy and the Importance of “Getting Away with It”», *Journal of Moral Philosophy* , 17 [2020]), pero esa no se encuentra entre las funciones más importantes de la privacidad.

[34] Carissa Véliz, «Inteligencia artificial. ¿Progreso o retroceso?», *El País* , 14 de junio de 2019.

[35] S. Zuboff, *The Age of Surveillance Capitalism* ..., pp. 221-225.

[36] Bent Flyvbjerg, *Rationality and Power. Democracy in Practice* , Chicago, The University of

Chicago Press, 1998, p. 36.

[37] Safiya Noble, *Algorithms of Oppression. How Search Engines Reinforce Racism* , Nueva York, New York University Press, 2018; Caroline Criado Perez, *Invisible Women. Exposing Data Bias in a World Designed for Men* , Londres, Vintage, 2019. [Hay trad. cast.: *La mujer invisible. Descubre cómo los datos configuran un mundo hecho por y para los hombres* , Barcelona, Seix Barral, 2020.]

[38] James Zou y Londa Schiebinger, «AI Can Be Sexist and Racist-It's Time to Make It Fair», *Nature* , 559 (2018).

[39] Danny Yadron, «Silicon Valley Tech Firms Exacerbating Income Inequality, World Bank Warns», *The Guardian* , 15 de enero de 2016.

[40] <https://www.energy.gov/articles/history-electric-car>.

[41] Nick Bilton, «Why Google Glass Broke», *The New York Times* , 4 de febrero de 2015.

[42] N. Bilton, «Why Google Glass Broke»...

[43] <https://about.fb.com/news/2020/09/announcing-projectaria-a-research-project-on-the-future-of-wearable-ar>.

[44] Steven Poole, «Drones the Size of Bees-Good or Evil?», *The Guardian* , 14 de junio de 2013.

[45] Rose Eveleth, «The Biggest Lie Tech People Tell Themselves— and the Rest of Us», *Vox* , 8 de octubre de 2019.

[46] J. Williams, *Stand Out of Our Light. ..*

[47] Gmail ya no analiza el contenido de nuestros mensajes de correo electrónico con fines de personalización publicitaria, pero lo hizo hasta 2017, y otras aplicaciones de terceros no han dejado de hacerlo (aunque podemos bloquear ese acceso si así lo indicamos en la página de configuración). Christopher Wylie, *Mindf*ck. Inside Cambridge Analytica's Plot to Break the World* , Londres, Profile Books, 2019, p. 15; Alex Hern, «Google Will Stop Scanning Content of Personal Emails», *The Guardian* , 26 de junio de 2017; Kaya Yurieff, «Google Still Lets Third-Party Apps Scan Your Gmail Data», *CNN Business* , 20 de septiembre de 2018.

[48] C. Wylie, *Mindf*ck* ..., p. 15.

[49] C. Wylie, *Mindf*ck* ..., p. 16.

[50] George Orwell, *Politics and the English Language* , Londres, Penguin, 2013. [Hay trad. cast.: «La política y la lengua inglesa», en *El poder y la palabra. Diez ensayos sobre lenguaje, política y verdad* , Barcelona, Debate, 2017.]

[51] «Nature's Language Is Being Hijacked by Technology», BBC News, 1 de agosto de 2019.

[52] C. Wylie, *Mindf*ck* ..., pp. 101-102.

[53] Facebook permitía también que miles de otros desarrolladores descargaran los datos de amigos de personas que sí habían consentido usar una app sin que los primeros lo supieran. Entre esos desarrolladores se incluían fabricantes de juegos como FarmVille, pero también Tinder y los organizadores de la campaña para las presidenciales de Barack Obama. Facebook modificó esa política en 2015. Elizabeth Dwoskin y Tony Romm, «Facebook's Rules for Accessing User Data Lured More than Just Cambridge Analytica», *The Washington Post* , 20 de marzo de 2018.

[54] C. Wylie, *Mindf*ck* ..., pp. 110-111.

[55] B. Kaiser, *Targeted* ..., caps. 9 y 3.

[56] C. Wylie, *Mindf*ck* ..., cap. 7.

[57] <https://www.channel4.com/news/cambridge-analytica-revea led-trumps-election-consultants-filmed-saying-they-use-bribes-and-sexworkers-to-entrap-politicians-investigation>.

[58] Alexander Nix (el director ejecutivo) y Mark Turnbull ofrecían algunos de esos servicios a una persona que creían que quería ser cliente suyo mientras eran grabados con cámara oculta por un equipo de Channel 4. Cambridge Analytica acusó luego a la cadena televisiva de incitación al delito y Nix aprovechó entonces la ocasión para rectificar sus propias palabras sobre las actividades que realizaba su empresa. Emma Graham-Harrison, Carole Cadwalladr y Hilary Osborne, «Cambridge Analytica Boasts of Dirty Tricks to Swing Elections», *The Guardian* , 19 de marzo de 2018, <https://www.theguardian.com/uk-news/2018/mar/19/cambridge-ana lytica-execs-boast-dirty-tricks-honey-traps-elections>. En fecha más

reciente, el Insolvency Service británico ha inhabilitado a Nix para la función de director de empresa durante siete años por haber tratado de vender a sus clientes los ya mencionados servicios «potencialmente contrarios a la ética». Rob Davies, «Former Cambridge Analytica Chief Receives Seven-Year Directorship Ban», *The Guardian* , 24 de septiembre de 2020.

[59] C. Wylie, *Mindf*ck* ..., cap. 8. La Information Commissioner's Office (ICO) del Reino Unido ha publicado hace poco un informe de su investigación sobre Cambridge Analytica. A juicio de algunos comentaristas, el documento exoneraba a la empresa de datos de tener vínculos con Rusia. Sin embargo, lo cierto es que la ICO solo constató allí que los asuntos relacionados con «una posible actividad localizada en Rusia» estaban fuera de su jurisdicción. Según otros comentaristas, sin embargo, parecía que la ICO estuviera negando que Cambridge Analytica hubiera estado implicada de forma activa en el referéndum del Brexit. Pero lo cierto es que en el informe se menciona la actividad de AggregateIQ (AIQ), una compañía con sede en Canadá vinculada con Cambridge Analytica y su sociedad matriz,SCL , que sí estuvo implicada en la campaña en favor de la salida de la Unión Europea. «The Observer View on the Information Commissioner's Cambridge Analytica Investigation», editorial, *The Observer* , 11 de octubre de 2020.

[60] C. Wylie, *Mindf*ck* ..., p. 244.

[61] Informe de la ICO (ICO /O /ED /L /RTL /0181), p.16: «A partir de las pruebas aportadas por los testigos, deducimos que AIQ desempeñó un papel significativo en el empleo de publicidad dirigida y se valió de sus conocimientos expertos en este tipo de *marketing* digital para ayudar a SCL . Un grupo de pruebas demostraba la existencia de una relación muy estrecha entre AIQ y SCL (entre ellas, había documentos en los que AIQ aparecía descrita como filial canadiense de SCL , y facturas de Facebook a AIQ en concepto de publicidad pagadas directamente por SCL). No obstante, AIQ ha negado de forma sistemática tener una relación más estrecha de la que pueda haber entre un desarrollador de software y su cliente. El señor Silvester (director/propietario de AIQ) ha declarado que, en 2014, SCL "nos pidió que creáramos SCL Canada, pero declinamos la oferta"».

[62] Amber Macintyre, «Who's Working for Your Vote?», *Tactical Tech* , 29 de noviembre de 2018.

[63] Lorenzo Franceschi-Bicchierai, «Russian Facebook Trolls Got Two Groups of People to Protest Each Other in Texas», *Motherboard* , 1 de noviembre de 2017.

[64] Gary Watson, «Moral Agency», en Hugh LaFollette (ed.), *The International Encyclopedia of Ethics* , Malden (Massachusetts), Wiley-Blackwell, 2013; John Christman, «Autonomy in Moral and Political Philosophy», en Edward N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* , 2015, <https://plato.stanford.edu/entries/autonomy-moral>.

[65] Myrna Oliver, «Legends Nureyev, Gillespie Die. Defector Was One of Century's Great Dancers», *Los Angeles Times* , 7 de enero de 1993.

[66] Jonathon W. Penney, «Chilling Effects. Online Surveillance and Wikipedia Use», *Berkeley Technology Law Journal* , 31 (2016).

[67] Karina Vold y Jess Whittlestone, «Privacy, Autonomy, and Personalised Targeting. Rethinking How Personal Data Is Used», en Carissa Véliz (ed.), *Data, Privacy, and the Individual* , Center for the Governance of Change, IE University, 2019.

[68] Hamza Shaban, «Google for the First Time Outspent Every Other Company to Influence Washington in 2019», *The Washington Post* , 23 de enero de 2018.

[69] Caroline Daniel y Maija Palmer, «Google's Goal. To Organise Your Daily Life», *Financial Times* , 22 de mayo de 2007.

[70] Holman W. Jenkins, «Google and the Search for the Future», *The Wall Street Journal* , 14 de agosto de 2010.

[71] Carissa Véliz, «Privacy Is a Collective Concern», *New Statesman* , 22 de octubre de 2019.

[72] Carissa Véliz, «Data, Privacy & the Individual», Center for the Governance of Change, IE University, 2020.

[73] K. V. Brown, «What DNA Testing Companies' Terrifying Privacy Policies Actually Mean»...

[74] Jody Allard, «How Gene Testing Forced Me to Reveal My Private Health Information», *Vice* , 27 de mayo de 2016.

[75] <https://blog.23andme.com/health-traits/sneezing-on-summersolstice>.

[76] S. L. Schilit y A. Schilit Nitenson, «My Identical Twin Sequenced Our Genome», *Journal of Genetic Counseling* , 16 (2017).

[77] Lydia Ramsey y Samantha Lee, «Our DNA is 99.9 % the Same as the Person Next to Us—and We're Surprisingly Similar to a Lot of Other Living Things», *Business Insider* , 3 de abril de 2018.

[78] Jocelyn Kaiser, «We Will Find You. DNA Search Used to Nab Golden State Killer Can Home In on about 60 % of White Americans», *Science Magazine* , 11 de octubre de 2018.

[79] Tamara Khandaker, «Canada Is Using Ancestry DNA Websites to Help It Deport People», *Vice News* , 26 de julio de 2018.

[80] J. Kaiser, «We Will Find You...».

[81] Matthew Shaer, «The False Promise of DNA Testing», *The Atlantic* , junio de 2016.

[82] Brendan I. Koerner, «Your Relative's DNA Could Turn You into a Suspect», *Wired* , 13 de octubre de 2015.

[83] Erin E. Murphy, *Inside the Cell. The Dark Side of Forensic DNA* , Nueva York, Nation Books, 2015.

[84] <https://www.innocenceproject.org/overturning-wrongful-con victions-involving-flawed-forensics>.

[85] Javier de la Cueva, comunicación personal.

[86] Keith Hampton, Lee Rainie, Weixu Lu, Maria Dwyer, Inyoung Shin y Kristen Purcell, «Social Media and the "Spiral of Silence"», Pew Research Center, 2014; Elizabeth Stoycheff, «Under Surveillance. Examining Facebook's Spiral of Silence Effects in the Wake of NSA Monitoring», *Journalism & Mass Communication Quarterly* , 93 (2016).

[87] Kieron O'Hara y Nigel Shadbolt, «Privacy on the Data Web», *Communications of the ACM* , 53 (2010).

[88] Robert B. Talisse, «Democracy. What's It Good for?», *The Philosophers' Magazine* , 89 (2020).

[89] «A Manifesto for Renewing Liberalism», *The Economist* , 13 de septiembre de 2018.

[90] Michael J. Abramowitz, «Freedom in the World. Democracy in Crisis», Freedom House, 2018.

[91] The Economist Intelligence Unit, «Democracy Index 2019. A Year of Democratic Setbacks and Popular Protest», 2019.

[92] «Democracy Under Lockdown», Freedom House, octubre de 2020, <https://freedomhouse.org/article/new-report-democracy-underlockdown-impact-covid-19-global-freedom>.

[93] <https://api.parliament.uk/historic-hansard/commons/1947/ nov/11/parliament-bill>.

[94] John Stuart Mill, *On Liberty* , Indianápolis, Hackett Publishing Company, 1978, cap. 3. [Hay trad. cast.: *Sobre la libertad* , Madrid, Alianza, 1984.]

[95] Agradezco a Mauricio Suárez el haberme recordado la teoría de la paz democrática, y a Antonio Diéguez el haber hecho lo mismo con el argumento de Karl Popper.

[96] Karl Popper, *The Open Society and Its Enemies* , Londres, Routledge, 2002, p. 368. [Hay trad. cast.: *La sociedad abierta y sus enemigos* , Barcelona, Paidós, 2006.]

[97] George Orwell, *Fascism and Democracy* , Londres, Penguin, 2020, p. 6.

[98] Steven Levitsky y Daniel Ziblatt, *How Democracies Die* , Londres, Penguin, 2018, p. 3. [Hay trad. cast.: *Cómo mueren las democracias* , Barcelona, Ariel, 2018.]

[99] Jonathan Wolff, «The Lure of Fascism», *Aeon* , 14 de abril de 2020.

[100] Hidalgo sostiene que deberíamos desprendernos de los representantes políticos y hacer que, en su lugar, sean nuestros asistentes digitales los que voten en nuestro nombre. Asegura que esta sería una forma de «democracia directa». Me parece un argumento muy cuestionable, pues se podría decir que lo único que está proponiendo es que sustituyamos a nuestros actuales representantes humanos por otros digitales. (Y no es que yo piense que la democracia directa es mejor que la representativa.) Véase <https://www.ted.com/talks/cesar_hidalgo_a_bold_idea_to_replace_politicians>.

[101] Sam Wolfson, «For My Next Trick. Dynamo's Mission to Bring Back Magic», *The Guardian* , 26 de abril de 2020.

[102] Cecilia Kang y Kenneth P. Vogel, «Tech Giants Amass a Lobbying Army for an Epic Washington

Battle», *The New York Times* , 5 de junio de 2019; Tony Romm, «Tech Giants Led by Amazon, Facebook and Google Spent Nearly Half a Billion on Lobbying over the Last Decade», *The Washington Post* , 22 de enero de 2020.

[103] Rana Foroohar, «Year in a Word. Techlash», *Financial Times* , 16 de diciembre de 2018.

4. Datos tóxicos

[1] Tom Douglas, «Why the Health Threat from Asbestos Is Not a Thing of the Past», *The Conversation* , 21 de diciembre de 2015.

[2] Bruce Schneier, «Data Is a Toxic Asset, So Why Not Throw It Out?», CNN , 1 de marzo de 2016.

[3] Tom Lamont, «Life after the Ashley Madison Affair», *The Observer* , 28 de febrero de 2016.

[4] Rob Price, «An Ashley Madison User Received a Terrifying Blackmail Letter», *Business Insider* , 22 de enero de 2016.

[5] Chris Baraniuk, «Ashley Madison.“Suicides” over Website Hack», BBC News, 24 de agosto de 2015; Laurie Segall, «Pastor Outed on Ashley Madison Commits Suicide», CNN , 8 de septiembre de 2015.

[6] José Antonio Hernández, «Me han robado la identidad y estoy a base de lexatín; yo no soy una delincuente», *El País* , 24 de agosto de 2016.

[7] Siân Brooke y Carissa Véliz, «Views on Privacy. A Survey», *Data, Privacy & the Individual* , Center for the Governance of Change, IE University, 2020.

[8] A. Hern, «Hackers Publish Private Photos from Cosmetic Surgery Clinic»...

[9] Zoe Kleinman, «Therapy Patients Blackmailed for Cash after Clinic Data Breach», BBC News, 26 de octubre de 2020.

[10] Isabel Valdés, «La Fiscalía investiga el suicidio de una empleada de Iveco tras la difusión de un vídeo sexual», *El País* , 30 de mayo de 2019.

[11] «How WhatsApp Helped Turn an Indian Village into a Lynch Mob», BBC News, 18 de julio de 2018.

[12] «Stalker “Found Japanese Singer through Reflection in Her Eyes”», BBC News, 10 de octubre de 2019.

[13] Kashmir Hill, «Wrongfully Accused by an Algorithm», *The New York Times* , 24 de junio de 2020.

[14] Oren Liebermann, «How a Hacked Phone May Have Led Killers to Khashoggi», CNN , 20 de enero de 2019.

[15] S. Brooke y C. Véliz, «Views on Privacy...».

[16] Olivia Solon, «Ashamed to Work in Silicon Valley. How Techies Became the New Bankers», *The Guardian* , 8 de noviembre de 2017.

[17] «FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook», *FTC Press Release* , 24 de julio de 2019.

[18] «Facebook Fined £500,000 for Cambridge Analytica Scandal»...

[19] «British Airways Faces Record £183m Fine for Data Breach», BBC News, 8 de Julio de 2019.

[20] David E. Sanger, «Hackers Took Fingerprints of 5.6 Million U. S. Workers, Government Says», *The New York Times* , 23 de septiembre de 2015.

[21] Edward Wong, «How China Uses LinkedIn to Recruit Spies Abroad», *The New York Times* , 27 de agosto de 2019.

[22] Jordi Pérez Colomé, «Por qué China roba datos privados de decenas de millones de estadounidenses», *El País* , 17 de febrero de 2020.

[23] En el sitio web dedicado específicamente a informar del acuerdo judicial para saldar su responsabilidad por el fallo de seguridad, la empresa señala que «Equifax negó haber realizado conducta delictiva alguna, y tampoco ha habido sentencia ni veredicto de culpabilidad en ese sentido», <https://www.equifaxbreachsettlement.com>. Equifax accedió a pagar 700 millones de dólares como una de

las condiciones del acuerdo al que llegó con la Comisión Federal de Comercio (FTC) de Estados Unidos. «Equifax no tomó medidas básicas que podrían haber evitado la violación de datos», declaró al respecto Joe Simons, presidente de la FTC . «Equifax to Pay Up to $700m to Settle Data Breach», BBC News, 22 de julio de 2019. Puede leerse el contenido de la demanda judicial colectiva interpuesta a Equifax en <http://securities.stanford.edu/filings-documents/1063/ EI00_15/2019128_r01x_17CV03463.pdf>.

[24] Charlie Warzel, «Chinese Hacking Is Alarming. So Are Data Brokers», *The New York Times* , 10 de febrero de 2020.

[25] Stuart A. Thompson y Charlie Warzel, «Twelve Million Phones, One Dataset, Zero Privacy», *The New York Times* , 19 de diciembre de 2019.

[26] Stuart A. Thompson y Charlie Warzel, «How to Track President Trump», *The New York Times* , 20 de diciembre de 2019.

[27] En el momento de escribir este capítulo, Oracle y Walmart han presentado una oferta conjunta por TikTok. Dado que Oracle es propietaria de más de ochenta brókeres de datos, con los que colabora, no parece que esta sea una buena noticia para la privacidad. Oracle asegura que vende datos sobre más de 300 millones de personas en todo el mundo, que posee unos treinta mil por individuo (datos referidos a su conducta de compras, a sus transacciones financieras, a su comportamiento en redes sociales, a su información demográfica, etcétera) y que su cobertura alcanza a «más del 80 por ciento del total de la población estadounidense en internet». A. Ram y M. Murgia, «Data Brokers...».

[28] Devin Coldewey, «Grindr Send HIV Status to Third Parties, and some Personal Data Unencrypted», *TechCrunch* , 2 de abril de 2018.

[29] Echo Wang y Carl O'Donnell, «Behind Grindr's Doomed Hookup in China, a Data Misstep and Scramble to Make Up», Reuters, 22 de mayo de 2019.

[30] Casey Newton, «How Grindr Became a National Security Issue», *Verge* , 28 de marzo de 2019.

[31] Jeremy Hsu, «The Strava Heat Map and the End of Secrets», *Wired* , 29 de enero de 2018.

[32] Colin Lecher, «Strava Fitness App Quietly Added a New Opt-Out for Controversial Heat Map», *Verge* , 1 de marzo de 2018.

[33] Pablo Guimón, «El Brexit no habría sucedido sin Cambridge Analytica», *El País* , 27 de marzo de 2018.

[34] Alex Hern, «Facebook "Dark Ads" Can Swing Political Opinions, Research Shows», *The Guardian* , 31 de julio de 2017; Timothy Revell, «How to Turn Facebook into a Weaponised AI Propaganda Machine», *New Scientist* , 28 de julio de 2017; Sue Halpern, «Cambridge Analytica and the Perils of Psychographics», *The New Yorker* , 30 de marzo de 2018.

[35] Angela Chen y Alessandra Potenza, «Cambridge Analytica's Facebook Data Abuse Shouldn't Get Credit for Trump», *Verge* , 20 de marzo de 2018; Kris-Stella Trump, «Four and a Half Reasons Not to Worry that Cambridge Analytica Skewed the 2016 Election», *The Washington Post* , 23 de marzo de 2018.

[36] Kyle Endres, «Targeted Issue Messages and Voting Behavior», *American Politics Research* , 48 (2020).

[37] En el artículo se explica que se llevó a cabo un ensayo controlado aleatorizado «con todos los usuarios mayores de edad de Estados Unidos que el 2 de noviembre de 2010 accedieron al sitio web de Facebook». Cabe suponer que Facebook asumió que ese estudio suyo estaba cubierto por sus propios términos y condiciones de uso de su plataforma (una suposición más que cuestionable). Parecida controversia se desató posteriormente, en 2014, cuando Facebook publicó un estudio sobre contagio emocional. La periodista Kashmir Hill señaló entonces que Facebook no había incluido entre sus términos hasta cuatro meses después de que realizara el mencionado estudio la posibilidad de que se usaran datos a efectos de sus propias investigaciones. Y tampoco parece que acceder a unos términos y condiciones que la mayoría de las personas no se leen pueda considerarse consentimiento informado. Kashmir Hill, «Facebook Added "Research" to User Agreement 4 Months after Emotion Manipulation Study», *Forbes* , 30 de junio de 2014.

[38] R. M. Bond, C. J. Fariss, J. J. Jones, A. D. Kramer, C. Marlow, J. E. Settle y J. H. Fowler, «A 61-Million-Person Experiment in Social Influence and Political Mobilization», *Nature* , 489 (2012).

[39] Jay Caruso, «The Latest Battlegoround Poll Tells Us Democrats Are Over-Correcting for 2020—

and They Can’t Beat Trump That Way», *The Independent* , 5 de noviembre de 2019.

[40] Channel 4 News, «Revealed. Trump Campaign Strategy to Deter Millions of Black Americans from Voting in 2016», YouTube, 28 de septiembre de 2020, <https://www.youtube.com/watch?v=KIf5ELaOjOk>.

[41] Hannes Grassegger, «Facebook Says Its “Voter Button” Is Good for Turnout. But Should the Tech Giant Be Nudging Us at All?», *The Observer* , 15 de abril de 2018.

[42] John Gramlich, «10 Facts about Americans and Facebook», Pew Research Center, 16 de mayo de 2019.

[43] YouTube, que es propiedad de Google y también se dedica al negocio de influir a las personas valiéndose de sus datos, es la única gran plataforma de red social usada por más estadounidenses todavía (un 73 por ciento).

[44] *Wired* contabilizó hasta 21 escándalos solo en 2018. Issie Lapowsky, «The 21 (and Counting) Biggest Facebook Scandals of 2018», *Wired* , 20 de diciembre de 2018.

[45] En 2019, Zuckerberg anunció que Facebook no moderaría ni verificaría el contenido de los anuncios políticos. Según fueron evolucionando los acontecimientos, Facebook recibió presiones para cambiar esa política y Zuckerberg transigió un poco. Facebook comenzó vetando anuncios que tuvieran como finalidad disuadir el ejercicio del derecho de voto. En fecha más reciente, la compañía prohibió también los anuncios políticos que pretendan «deslegitimar unas elecciones», incluidos los que incluyan alegaciones injustificadas de fraude electoral. La plataforma también ha decidido ahora prohibir por tiempo indefinido la totalidad de los anuncios políticos en cuanto se proceda al cierre de los colegios electorales el 3 de noviembre. Aunque se trata de políticas positivas, no tenemos garantía alguna de que se lleven a la práctica de un modo fiable, ni tampoco de que vayan a bastar para garantizar el juego limpio en Facebook. Cecilia Kang y Mike Isaac, «Defiant Zuckerberg Says Facebook Won’t Police Political Speech», *The New York Times* , 17 de octubre de 2019; Hannah Murphy, «Facebook to Ban Ads That Aim to “Delegitimise an Election”», *Financial Times* , 1 de octubre de 2020.

[46] Tim Wu, «Facebook Isn’t Just Allowing Lies, It’s Prioritizing Them», *The New York Times* , 4 de noviembre de 2019; Donie O’Sullivan y Brian Fung, «Facebook Will Limit some Advertising in the Week before the US Election—but It Will Let Politicians Run Ads with Lies», *CNN Business* , 3 de septiembre de 2020.

[47] Andrew Marantz, «Why Facebook Can’t Fix Itself», *The New Yorker* , 12 de octubre de 2020.

[48] Karen Kornbluh, Adrienne Goldstein y Eli Weiner, «New Study by Digital New Deal Finds Engagement with Deceptive Outlets Higher on Facebook Today than Run-Up to 2016 Election», German Marshall Fund of the United States, 12 de octubre de 2020.

[49] David Smith, «How Key Republicans inside Facebook Are Shifting Its Politics to the Right», *The Guardian* , 3 de noviembre de 2019.

[50] Jonathan Zittrain, «Facebook Could Decide an Election without Anyone Ever Finding Out», *New Statesman* , 3 de junio de 2014.

[51] Chris Wylie y Brittany Kaiser, denunciantes internos, aseguran que Cambridge Analytica impulsó la disuasión del ejercicio del derecho de voto de ciertos sectores del electorado. O’Sullivan y Drew Griffin, «Cambridge Analytica Ran Voter Suppression Campaigns, Whistleblower Claims», *CNN Politics* , 17 de mayo de 2018; B. Kaiser, *Targeted* ..., p. 231

[52] Ante los llamamientos a una mayor transparencia, Facebook abrió una biblioteca en línea de todos los anuncios existentes en su plataforma. No obstante, varios periodistas e investigadores se han quejado de que es una herramienta «tan plagada de fallos y limitaciones técnicas que, en la práctica, es inútil como método de seguimiento exhaustivo de la publicidad política». Matthew Rosenberg, «Ad Tool Facebook Built to Fight Disinformation Doesn’t Work as Advertised», *The New York Times* , 25 de julio de 2019.

[53] John Stuart Mill, *Collected Works of John Stuart Mill* , University of Toronto Press, 1963, t. 21, p. 262.

[54] Thomas Nagel, «Concealment and Exposure», *Philosophy and Public Affairs* , 27 (1998).

[55] Anna Lauren Hoffman, «Facebook Is Worried about Users Sharing Less—but It Only Has Itself to Blame», *The Guardian* , 19 de abril de 2016.

[56] T. Nagel, «Concealment and Exposure»..., p. 7.

[57] Edwin Black, *IBM and the Holocaust* , Washington, Dialog Press, 2012, cap. 11. [Hay trad. cast.: *IBM y el Holocausto* , Buenos Aires, Atlántida, 2001.]

[58] William Seltzer y Margo Anderson, «The Dark Side of Numbers. The Role of Population Data Systems in Human Rights Abuses», *Social Research* , 68 (2001).

[59] W. Seltzer y M. Anderson, «The Dark Side of Numbers...».

[60] Teniendo en cuenta esta turbia historia de los carnets de identidad, resulta comprensible que Reino Unido decidiera abolirlos en 1952, como también son de entender las reticencias expresadas en los debates recientes que se han suscitado a raíz de que se planteara la posibilidad de recuperarlos.

[61] Hans de Zwart, «During World War II, We Did Have Something to Hide», *Medium* , 30 de abril de 2015.

[62] Thomas Douglas y Laura Van den Borre, «Asbestos Neglect. Why Asbestos Exposure Deserves Greater Policy Attention», *Health Policy* , 123 (2019).

5. Desenchufar

[1] Fiona Harvey, «Ozone Layer Finally Healing after Damage Caused by Aerosols, UN Says», *The Guardian* , 5 de noviembre de 2018.

[2] «Update Report into Adtech and Real Time Bidding», Information Commissioner's Office (ICO) (Reino Unido), 2019.

[3] Jesse Frederik y Maurits Martijn, «The New Dot Com Bubble Is Here:It's Called Online Advertising», *The Correspondent* ,6 de noviembre de 2019.

[4] Keach Hagey, «Behavioral Ad Targeting Not Paying Offfor Publishers, Study Suggest», *The Wall Street Journal* , 29 de mayo de 2019.

[5] Laura Bassett, «Digital Media Is Suffocating—and It's Facebook and Google's Fault», *The American Prospect* , 6 de mayo de 2019.

[6] Natasha Lomas, «The Case against Behavioral Advertising Is Stacking Up», *TedCrunch* , 20 de enero de 2019.

[7] De todos modos, merece la pena que tengamos en cuenta que, si bien los anuncios dirigidos no valen lo que cuestan, las grandes plataformas pueden proporcionar acceso a un público tan numeroso que, aun así, a los anunciantes les puede seguir interesando hacer uso de ellas.

[8] Mark Weiss, «Digiday Research. Most Publishers Don't Benefit from Behavioral Ad Targeting», *Digiday* , 5 de junio de 2019.

[9] Jessica Davies, «After GDPR , *The New York Times* Cut OffAd Exchanges in Europe—and Kept Growing Ad Revenue», *Digiday* , 16 de enero de 2019.

[10] Tiffany Hsu, «The Advertising Industry Has a Problem. People Hate Ads», *The New York Times* , 28 de octubre de 2019.

[11] David Ogilvy, *Confessions of an Advertising Man* , Harpenden (Reino Unido), Southbank Publishing, 2013, pp. 17 y 114. [Hay trad. cast.: *Confesiones de un publicitario* , Barcelona, Oikos-Tau, 1965.]

[12] Louise Matsakis, «Online Ad Targeting Does Work—as Long as It's Not Creepy», *Wired* , 11 de mayo de 2018; Tami Kim, Kate Barasz y Leslie K.John, «Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness», *Journal of Consumer Research* , 45 (2019).

[13] Rani Molla, «These Publications Have the Most to Lose from Facebook's New Algorithm Changes», *Vox* , 25 de enero de 2018.

[14] Emily Bell, «Why Facebook's News Feed Changes Are Bad News for Democracy», *The Guardian* , 21 de enero de 2018; Dom Phillips, «Brazil's Biggest Newspaper Pulls Content from Facebook after Algorithm Change», *The Guardian* , 8 de febrero de 2018.

[15] Gabriel Weinberg, «What if We All Just Sold Non-Creepy Advertising?», *The New York Times* , 19

de junio de 2019.

[16] D. Ogilvy, *Confessions of an Advertising Man* ..., pp. 168, 112 y 127.

[17] Chloé Michel, Michelle Sovinsky, Eugenio Proto y Andrew Oswald, «Advertising as a Major Source of Human Dissatisfaction. Cross-National Evidence on One Million Europeans», en Mariano Rojas (ed.), *The Economics of Happiness* , Nueva York, Springer, 2019.

[18] «Economic Impact of Advertising in the United States»,IHS Economics and Country Risk, 2015.

[19] Knoema, «United States of America—Contribution of Travel and Tourism to GDP as a Share of GDP », 2018.

[20] Schumpeter, «Something Doesn't Ad Up about America's Advertising Market», *The Economist* , 18 de enero de 2018.

[21] Eli Rosenberg, «Quote. The Ad Generation», *The Atlantic* , 15 de abril de 2011.

[22] Schumpeter, «Something Doesn't Ad Up about America's Advertising Market»...

[23] Robert O'Harrow Jr., «Online Firm Gave Victim's Data to Killer», *Chicago Tribune* , 6 de enero de 2006.

[24] N. Singer, «Data Broker Is Charged with Selling Consumers' Financial Details to "Fraudsters"»...

[25] David A. Hoffman, «Intel Executive: Rein In Data Brokers», *The New York Times* , 15 de julio de 2019.

[26] Elizabeth Dwoskin, «FTC . Data Brokers Can Buy Your Bank Account Number for 50 Cents», *The Wall Street Journal* , 24 de diciembre de 2014; Julia Angwin, *Dragnet Nation* , Nueva York, Times Books, 2014, p. 7.

[27] Joana Moll, «The Dating Brokers. An Autopsy of Online Love», octubre de 2018, <https://datadating.tacticaltech.org/viz>.

[28] Alex Hern, «Apple Contractors "Regularly Hear Confidential Details" on Siri Recordings», *The Guardian* , 26 de julio de 2019; Alex Hern, «Facebook Admits Contractors Listened to Users? Recordings without Their Knowledge», *The Guardian* , 14 de agosto de 2019; Joseph Cox, «Revealed. Microsoft Contractors Are Listening to some Skype Calls», *Motherboard* , 7 de agosto de 2019; Austin Carr, Matt Day, Sarah Frier y Mark Gurman, «Silicon Valley Is Listening to Your Most Intimate Moments», *Bloomberg Businessweek* , 11 de diciembre de 2019; Alex Hern, «Apple Whistleblower Goes Public over "Lack of Action"», *The Guardian* , 20 de mayo de 2020.

[29] Nigel Shadbolt y Roger Hampson, *The Digital Ape. How to Live (in Peace) with Smart Machines* , Oxford, Oxford University Press, 2019, p. 318.

[30] G. J. X. Dance, M. LaForgia y N. Confessore, «As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants»...

[31] S. Zuboff, *The Age of Surveillance Capitalism* ..., pp. 138-155.

[32] Este es un ejemplo que he sacado de una entrevista que mantuve con Aaron Roth (él usó la campaña de Trump para ilustrar el método), <https://twimlai.com/twiml-talk-132-differential-privacy-theory-practice-with-aaron-roth>.

[33] Rachel Metz, «The Smartphone App That Can Tell You're Depressed before You Know It Yourself», *MIT Technology Review* , 15 de octubre de 2018.

[34] Michal Kosinski, David Stillwell y Thore Graepel, «Private Traits and Attributes Are Predictable from Digital Records of Human Behavior», *Proceedings of the National Academy of Sciences (PNAS)* , 110 (2013).

[35] Christopher Burr y Nello Cristianini, «Can Machines Read Our Minds?», *Minds and Machines* , 29 (2019).

[36] M. Kosinski, D. Stillwell y T. Graepel, «Private Traits and Attributes Are Predictable from Digital Records of Human Behavior»...

[37] Alexis Kramer, «Forced Phone Fingerprint Swipes Raise Fifth Amendment Questions», *Bloomberg Law* , 7 de octubre de 2019.

[38] Jack M. Balkin, «Information Fiduciaries and the First Amendment», *UC Davis Law Review* , 49 (2016); Jonathan Zittrain, «How to Exercise the Power You Didn't Ask for», *Harvard Business Review* , 19

de septiembre de 2018.

[39] Alice MacLachlan, «Fiduciary Duties and the Ethics of Public Apology», *Journal of Applied Philosophy* , 35 (2018), p. 366.

[40] Lina Khan y David E. Pozen, «A Skeptical View of Information Fiduciaries», *Harvard Law Review* , 133, (2019), p. 530.

[41] B. Schneier, *Click Here to Kill Everybody* ..., p. 134.

[42] Andy Greenberg, «How Hacked Water Heaters Could Trigger Mass Blackouts», *Wired* , 13 de agosto de 2018. Rusia provocó un apagón general en Ucrania en 2016 por medio de un ciberataque. Andy Greenberg, «New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction», *Wired* , 12 de septiembre de 2019.

[43] Sean Lyngaas, «Hacking Nuclear Systems Is the Ultimate Cyber Threat. Are We Prepared?», *Verge* , 23 de enero de 2018.

[44] Will Dunn, «Can Nuclear Weapons Be Hacked?», *New Statesman* , 7 de mayo de 2018. Estados Unidos e Israel obstruyeron el desarrollo del programa nuclear iraní lanzando un ciberataque (Stuxnet). Ellen Nakashima y Joby Warrick, «Stuxnet Was Work of US and Israeli Experts, Officials Say», *The Washington Post* , 2 de junio de 2012. Más preocupante todavía sería un ataque dirigido a activar un arma nuclear.

[45] Matthew Wall, «5G."A Cyber-Attack Could Stop the Country"», BBC News, 25 de octubre de 2018.

[46] En una viñeta de Paul Noth publicada en *The New Yorker* , un grupo de sórdidos personajes están sentados en torno a una mesa. Uno de ellos tiene una pistola y dice: «Por motivos de salud y de seguridad, procederemos a hacer una transición hacia la ciberdelincuencia».

[47] Jillian Ambrose, «Lights Stay On Despite Cyber-Attack on UK'S Electricity System», *The Guardian* , 14 de mayo de 2020.

[48] «WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance», <https://www.who.int/news-room/detail/23-04-2020-whoreports-fivefold-increase-in-cyber-attacks-urges-vigilance>.

[49] B. Schneier, *Click Here to Kill Everybody* ..., pp. 118-119.

[50] B. Schneier, *Click Here to Kill Everybody* ..., pp. 32-33 y 168; K. Zetter, «How Cops Can Secretly Track Your Phone»...

[51] Gary Marcus, «Total Recall. The Woman Who Can't Forget», *Wired* , 23 de marzo de 2009.

[52] Viktor Mayer-Schönberger, *Delete. The Virtue of Forgetting in the Digital Age* , Princeton (Nueva Jersey), Princeton University Press, 2009, pp. 39-45.

[53] V. Mayer-Schönberger, *Delete* ..., cap. 4.

[54] He tomado este ejemplo del análisis que hicieron Carl Bergstrom y Jevin West de un trabajo publicado en el que se decía que un algoritmo es capaz de determinar si alguien es un delincuente solo con analizar una imagen del rostro de esa persona. «Criminal Machine Learning», <https://callingbullshit.org/case_studies/case_study_criminal_machine_learning.html>.

[55] Julia Powles y Enrique Chaparro, «How Google Determined Our Right to Be Forgotten», *The Guardian* , 18 de febrero de 2015.

[56] Jack Nicas, «The Police Can Probably Break into Your Phone», *The New York Times* , 21 de octubre de 2020.

[57] Estas y otras buenas sugerencias figuran en B. Schneier, *Data and Goliath* ..., cap. 13.

[58] David Cole, «"We Kill People Based on Metadata"», *The New York Review of Books* , 10 de mayo de 2014.

[59] Evan Selinger y Woodrow Hartzog, «What Happens When Employers Can Read Your Facial Expressions?», *The New York Times* , 17 de octubre de 2019; Woodrow Hartzog y Evan Selinger, «Facial Recognition Is the Perfect Tool for Oppression», *Medium* , 2 de agosto de 2018; David Hambling, «The Pentagon Has a Laser That Can Identify People from a Distance—by Their Heartbeat», *MIT Technology Review* , 27 de junio de 2019.

[60] Tom Miles, «UN Surveillance Expert Urges Global Moratorium on Sale of Spyware», Reuters, 18 de junio de 2019.

[61] Nick Hopkins y Stephanie Kirchgaessner, «WhatsApp Sues Israeli Firm, Accusing It of Hacking Activists' Phones», *The Guardian* , 29 de octubre de 2019.

[62] Sarah Parcak, «Are We Ready for Satellites That See Our Every Move?», *The New York Times* , 15 de octubre de 2019.

[63] Amy Maxmen, «Surveillance Science», *Nature* , 569 (2019).

[64] «The Mission to Create a Searchable Database of Earth's Surface», <https://www.ted.com/talks/will_marshall_the_mission_to_create_a_searchable_database_of_earth_s_surface>.

[65] James Vincent, «iRobot's Latest Roomba Remembers Your Home's Layout and Empties Itself», *Verge* , 6 de septiembre de 2018.

[66] Evan Ackerman, «Why You Should Be Very Skeptical of Ring's Indoor Security Drone», *IEEE Spectrum* , 25 de septiembre de 2020.

[67] Véase <https://about.fb.com/news/2020/09/announcingproject-aria-a-research-project-on-the-future-of-wearable-ar>.

[68] Adam Satariano, «Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates», *The New York Times* , 27 de abril de 2020.

[69] Steve Lohr, «Forget Antitrust Laws. To Limit Tech, Some Say a New Regulator Is Needed», *The New York Times* , 22 de octubre de 2020.

[70] Dos cosas que me han llevado a ser especialmente consciente de la importancia de la diplomacia en este terreno han sido una conversación que mantuvimos en línea Tom Fletcher, Zeid Ra'ad, Mike Wooldridge y yo, así como el libro de Tom Fletcher *The Naked Diplomat* , Londres, William Collins, 2017. Véase la conversación en <https://www.youtube.com/watch?v=LnV8iU0CLpg>.

[71] Carissa Véliz, «You've Heard of Tax Havens. After Brexit, the UK Could Become a "Data Haven"», *The Guardian* , 17 de octubre de 2020.

[72] Lois Beckett, «Under Digital Surveillance. How American Schools Spy on Millions of Kids», *The Guardian* , 22 de octubre de 2019.

[73] Tristan Louis, «How Much Is a User Worth?», *Forbes* , 31 de agosto de 2013.

[74] James H. Wilson, Paul R. Daugherty y Chase Davenport, «The Future of AI Will Be about Less Data, Not More», *Harvard Business Review* , 14 de enero de 2019.

[75] Bruce Schneier y James Waldo, «AI Can Thrive in Open Societies», *Foreign Policy* , 13 de junio de 2019.

[76] Eliza Strickland, «How IBM Watson Overpromised and Underdelivered on AI Health Care», *IEEE Spectrum* , 2 de abril de 2019.

[77] Martin U. Müller, «Medical Applications Expose Current Limits of AI », *Der Spiegel* , 3 de agosto de 2018.

[78] Angela Chen, «IBM 's Watson Gave Unsafe Recommendations for Treating Cancer», *Verge* , 26 de julio de 2018.

[79] Hal Hodson, «Revealed. Google AI Has Access to Huge Haul of NHS Patient Data», *New Scientist* , 29 de abril de 2016.

[80] La ICO dictaminó que el ensayo de Royal Free y DeepMind había incumplido la ley sobre protección de datos: <https://ico.org.uk/aboutthe-ico/news-and-events/news-and-blogs/2017/07/royal-free-googledeepmind-trial-failed-to-comply-with-data-protection-law>.

[81] Julia Powles, «DeepMind's Latest AI Health Breakthrough Has some Problems», *Medium* , 6 de agosto de 2019.

[82] Xiaoxuan Liu, Livia Faes, Aditya U. Kale, Siegfried K. Wagner, Dun Jack Fu, Alice Bruynseels, Thushika Mahendiran, Gabriella Moraes, Mohith Shamdas, Christoph Kern, Joseph R. Ledsam, Martin K. Schmid, Konstantinos Balaskas, Eric J. Topol, Lucas M. Machmann, Pearse A. Keane y Alastair K. Denniston, «A Comparison of Deep Learning Performance against Health-Care Professionals in Detecting Diseases from Medical Imaging. A Systematic Review and Meta-Analysis», *Lancet Digital Health* , 1 (2019).

[83] L. Wang, L. Ding, Z. Liu, L. Sun, L. Chen, R. Jia, X. Dai, J. Cao y J. Ye, «Automated Identification of Malignancy in Whole-Slide Pathological Images. Identification of Eyelid Malignant Melanoma in Gigapixel Pathological Slides Using Deep Learning», *British Journal of Ophthalmology* , 104 (2020).

[84] Margi Murphy, «Privacy Concerns as Google Absorbs DeepMind's Health Division», *The Telegraph* , 13 de noviembre de 2018.

[85] J. Powles y H. Hodson, «Google DeepMind and Healthcare in an Age of Algorithms»...

[86] En el momento de escribir estas líneas, no está aún claro si la pandemia de coronavirus se cobrará suficientes vidas como para convertirse en la excepción a la regla de que la mayoría de la población fallece de enfermedades no transmisibles.

[87] Anne Trafton, «Artificial Intelligence Yields New Antibiotic», MIT News Office, 20 de febrero de 2020.

[88] En julio de 2020, *The New York Times* informó de que, aunque Apple y Google habían prometido privacidad para los usuarios de apps de rastreo de contactos basadas en su interfaz de programación de aplicaciones, para que estas funcionaran en Android los usuarios debían activar la opción de detección de la ubicación del dispositivo, que enciende a su vez el GPS , aunque las aplicaciones en sí usen solamente el *bluetooth* . El GPS es más invasivo que el *bluetooth* porque registra la ubicación. Se teme que Google pueda aprovechar la situación para recopilar y rentabilizar en provecho propio los datos de ubicación de los usuarios. Natasha Singer, «Google Promises Privacy with Virus App but Can Still Collect Location Data», *The New York Times* , 20 de julio de 2020. En julio, Google actualizó la interfaz de programación de aplicaciones. Ahora, quienes tengan teléfonos con Android 11 podrán usar las aplicaciones sin activar la opción de detección de ubicación del dispositivo. De todos modos, continúa siendo necesario poner en marcha esa función para que la app funcione en versiones anteriores del sistema operativo. Véase <https://blog.google/inside-google/company-an nouncements/update-exposure-notifications>.

[89] Lorenzo Tondo, «Scientists Say Mass Tests in Italian Town Have Halted Covid-19 There», *The Guardian* , 18 de marzo de 2020.

[90] «Covid-19. China's Qingdao to Test Nine Million in Five Days», BBC News, 12 de octubre de 2020.

[91] Yves-Alexandre de Montjoye y su equipo han publicado una entrada de blog sobre los que, a su juicio, son los mayores riesgos de las aplicaciones de rastreo del coronavirus. Yves-Alexandre de Montjoye, Florimond Houssiau, Andrea Gadotti y Florent Guepin, «Evaluating COVID-19 Contact Tracing Apps? Here Are 8 Privacy Questions We Think You Should Ask», Computational Privacy Group, 2 de abril de 2020, <https://cpg.doc. ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-ques tions-we-think-you-should-ask>.

[92] Véase <https://www.youtube.com/watch?v=_mzcbXi1Tkk>.

[93] Naomi Klein, *The Shock Doctrine* , Toronto, Random House, 2007. [Hay trad. cast.: *La doctrina del shock* , Barcelona, Paidós, 2007.]

[94] Paul Mozur, Raymond Zhong y Aaron Krolik, «In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags», *The New York Times* , 1 de marzo de 2020.

[95] Shanti Das y Shingi Mararike, «Contact-Tracing Data Harvested from Pubs and Restaurants Being Sold On», *The Times* , 11 de octubre de 2020.

[96] Naomi Klein, «Screen New Deal», *The Intercept* , 8 de mayo de 2020.

[97] N. Klein, «Screen New Deal»...

[98] Oscar Williams, «Palantir's NHS Data Project "May Outlive Coronavirus Crisis"», *New Statesman* , 30 de abril de 2020.

[99] Nick Statt, «Peter Thiel's Controversial Palantir Is Helping Build a Coronavirus Tracking Tool for the Trump Admin», *Verge* , 21 de abril de 2020.

[100] Amy Thomson y Jonathan Browning, «Peter Thiel's Palantir Is Given Access to U. K. Health Data on Covid-19 Patients», *Bloomberg* , 5 de junio de 2020.

[101] João Carlos Magalhães y Nick Couldry, «Tech Giants Are Using This Crisis to Colonize the Welfare System», *Jacobin* , 27 de abril de 2020.

[102] Jon Henley y Robert Booth, «Welfare Surveillance System Violates Human Rights, Dutch Court

Rules», *The Guardian* , 5 de febrero de 2020.

[103] Yuval Harari, «The World after Coronavirus», *Financial Times* , 20 de marzo de 2020.

[104] «Big Tech's $2trn Bull Run», *The Economist* , 22 de febrero de 2020.

[*] Si tienes un dispositivo *wearable* , piensa que está monitorizando, registrando y analizando tu ritmo cardiaco durante todo el día, y de ahí puede inferirse tu actividad sexual. En 2019, *Bloomberg* , *The Guardian* y *Vice News* revelaron que Amazon, Google, Facebook, Microsoft y Apple llevan ya tiempo contratando a personal humano para que analice grabaciones de los asistentes de voz. Algunos de estos analistas contratados admitieron haber escuchado en ocasiones a personas manteniendo relaciones sexuales. Un denunciante interno de Apple dijo: «He oído a gente hablando de su cáncer, o de sus parientes muertos, de religión, de sexualidad, de pornografía, de política, de los estudios, de relaciones o de drogas, sin que antes hubieran activado Siri ni lo hubieran pretendido siquiera».

6. Lo que puedes hacer

[1] Carissa Véliz, «Why You Might Want to Think Twice about Surrendering Online Privacy for the Sake of Convenience», *The Conversation* , 11 de enero de 2017.

[2] Chris Wood, «WhatsApp Photo Drug Dealer Caught by "Groundbreaking" Work», BBC News, 15 de abril de 2018; Zoe Kleinman, «Politician's Fingerprint "Cloned from Photos" by Hacker», BBC News, 29 de diciembre de 2014.

[3] Leo Kelion, «Google Chief. I'd Disclose Smart Speakers before Guests Enter My Home», BBC News, 15 de octubre de 2019.

[4] En Países Bajos, un tribunal ha ordenado que una abuela borre todas las fotos de sus nietos que publicó en Facebook sin permiso de los padres de estos. «Grandmother Ordered to Delete Facebook Photos under GDPR », BBC News, 21 de mayo de 2020.

[5] Sonia Bokhari, «I'm 14, and I Quit Social Media after Discovering What Was Posted about Me», *Fast Company* , 18 de marzo de 2019.

[6] Sara Salinas, «Six Top US Intelligence Chiefs Caution against Buying Huawei Phones», CNBC , 13 de febrero de 2018.

[7] Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador y Narseo Vallina-Rodríguez, «An Analysis of Pre-Installed Android Software», *41st IEEE Symposium on Security and Privacy* , 2019.

[8] Parmy Olson, «Exclusive. WhatsApp Cofounder Brian Acton Gives the Inside Story on #DeleteFacebook and Why He Left $850 Million Behind», *Forbes* , 26 de septiembre de 2018.

[9] William Turton, «Why You Should Stop Using Telegram Right Now», *Gizmodo* , 24 de junio de 2016.

[10] Gracias a Ian Preston por haberme enseñado este truco.

[11] Véase <https://blog.mozilla.org/security/2020/02/06/multiaccount-containers-sync>.

[12] T. J. McCue, «47 Percent of Consumers Are Blocking Ads», *Forbes* , 19 de marzo de 2019.

[13] C. Wylie, *Mindf*ck* ..., p. 114.

[14] Kim Zetter, «The NSA Is Targeting Users of Privacy Services, Leaked Code Shows», *Wired* , 3 de julio de 2014.

[15] Kate O'Flaherty, «Facebook Shuts Its Onavo Snooping App—but It Will Continue to Abuse User Privacy», *Forbes* , 22 de febrero de 2019.

[16] Estas son algunas guías para iniciarte, aunque tal vez te interese comprobar antes si ya hay algunas más actualizadas en línea: Ntiva, Inc., «The Default Privacy Settings You Should Change and How to Do It», *Medium* , 18 de julio de 2018; J. R. Raphael, «7 Google Privacy Settings You Should Revisit Right Now», *Fast Company* , 17 de mayo de 2019; Preston Gralla, «How to Protect Your Privacy on Facebook», *Verge* , 7 de junio de 2019.

[17] Alex Hern, «Are You A "Cyberhoarder"? Five Ways to Declutter Your Digital Life—from Emails to Photos», *The Guardian* , 10 de octubre de 2018.

[18] K. G. Orphanides, «How to Securely Wipe Anything from Your Android, iPhone or PC », *Wired* , 26 de enero de 2020.

[19] Puede verse una lista de las diez mil contraseñas más habituales (y que deberías evitar) en <https://en.wikipedia.org/wiki/Wikipedia: 10,000_most_common_passwords>.

[20] Finn Brunton y Helen Nissenbaum, *Obfuscation. A User's Guide for Privacy and Protest* , Cambridge (Massachusetts), MIT Press, 2015, p. 1.

[21] Alfred Ng, «Teens Have Figured Out How to Mess with Instagram's Tracking Algorithm», CNET , 4 de febrero de 2020.

[22] Hilary Osborne, «Smart Appliances May Not Be Worth Money in Long Run, Warns Which?», *The Guardian* , 8 de junio de 2020.

[23] Véase <https://privacyinternational.org/mydata>.

[24] E. Black, *IBM and the Holocaust.* ..

[25] Por ejemplo, con relación a la persecución de los rohinyás, Facebook ya ha admitido no «haber hecho lo suficiente para impedir» que se usara su plataforma «para fomentar la división e incitar a la violencia fuera de internet». Una misión enviada por la ONU a Birmania para investigar lo sucedido allí señaló a Facebook por haber sido un «instrumento útil en manos de quienes pretendían sembrar el odio». Muchos miles de personas han sido asesinados. Hannah Ellis-Petersen, «Facebook Admits Failings over Incitement to Violence in Myanmar», *The Guardian* , 6 de noviembre de 2018; «Myanmar Rohingya. Why Facebook Banned an Army Chief», BBC News, 18 de agosto de 2018.

[26] Jack Poulson, «Tech Needs More Conscientious Objectors», *The New York Times* , 23 de abril de 2019.

[27] En Reino Unido, Digital Catapult ofrece este tipo de servicio (y ya aviso de que actualmente soy miembro de su comité de ética).

[28] Anna Wiener, «Taking Back Our Privacy», *The New Yorker* , 19 de octubre de 2020.

[29] Si Apple pone en práctica las protecciones de la privacidad que ha prometido, Facebook se verá presionado a cambiar algunas de sus prácticas invasivas de la intimidad. Megan Graham, «Facebook Revenue Chief Says Ad-Supported Model Is "under Assault" amid Apple Privacy Changes», CNBC , 6 de octubre de 2020.

[30] Andy Greenberg, «A Guide to Getting Past Customs with Your Digital Privacy Intact», *Wired* , 12 de febrero de 2017.

[31] Stéphane Hessel, *The Power of Indignation* , Nueva York, Skyhorse Publishing, 2012.

[32] «The Data Economy. Special Report», *The Economist* , 20 de febrero de 2020.

Conclusión

[1] Y. Harari, «The World after Coronavirus»...

«Para viajar lejos no hay mejor nave que un libro.»

EMILY DICKINSON

Gracias por tu lectura de este libro.

En **Penguinlibros.club** encontrarás las mejores recomendaciones de lectura.

Únete a nuestra comunidad y viaja con nosotros.

Penguinlibros.club

Penguin Random House Grupo Editorial

Penguinlibros

Índice

Privacidad es poder. Datos, vigilancia y libertad en la era digital

Introducción
1. Buitres de datos
2. ¿Cómo hemos llegado a esto?
3. Privacidad es poder
4. Datos tóxicos
5. Desenchufar
6. Lo que puedes hacer
Conclusión
Bibliografía
Agradecimientos

Sobre este libro
Sobre Carissa Véliz
Créditos
Notas