Privacidad en un mundo digital. Comentario a Carissa Véliz, Privacy is power: why and how you should take back control of your data*

(2020) Bantam Press,
London, 268 pp.

Isabel Turégano Mansilla
Universidad de Castilla-La Mancha
ORCID ID 0000-0003-1980-4351
isabel.turegano@uclm.es

Cita recomendada:

Turégano Mansilla, I. (2021). Privacidad en un mundo digital. Comentario a Carissa Véliz, Privacy is power: why and how you should take back control of your data. *Eunomía. Revista en Cultura de la Legalidad*, 21, pp. 407-426.

doi: https://doi.org/10.20318/eunomia.2021.6364

Recibido / received: 13/08/2021

Mientras escribo este comentario leo en la prensa que el Director del *StratCom* (Centro de Comunicación Estratégica de la OTAN) afirma que el manejo de los datos será una amenaza a la seguridad nacional en el futuro. Janis Sarts alerta de que el uso malicioso de datos personales accesibles o que pueden ser comprados representa un arma que amenaza la seguridad de nuestras democracias (Domínguez Cebrián, 2021). Pocos días después se nos informa de que la Agencia Tributaria española emplea el *big data* para detectar el fraude fiscal. La Agencia puede controlar el patrimonio de personas deslocalizadas, usando mecanismos de análisis sofisticado para investigar y comprender complejos entramados financieros y societarios (González, 2021). Las cantidades ingentes de datos que cada día se generan y almacenan con las tecnologías digitales pueden verse tanto como un riesgo grave a nuestro modelo liberal y democrático de organización social, como una oportunidad para innovar económicamente y mejorar la prestación de servicios públicos. En ambos casos, sin embargo, se asume que la privacidad tiene una dimensión social

* Este trabajo se ha realizado en el marco del "Construcción de derechos emergentes. Debates para la fundamentación de nuevos parámetros de constitucionalidad [CDREM]" (PID2019-106904RB-I00 / AEI / 10.13039/501100011033), financiado por la Agencia Estatal de Investigación.

sobre la que es esencial deliberar en nuestros días para decidir qué modelo económico y político queremos para nuestras sociedades.

El libro de Carissa Véliz, que aparece en castellano este otoño, es una lúcida reflexión desde la filosofía que nos alerta de los riesgos del modelo cultural y económico de datos que hemos permitido que se haya implantado. Aunque llama a la acción individual y social comprometida, su obra es también un alegato en favor de una intervención más garantista del Derecho. Hemos asumido acríticamente un modelo social y económico basado en la compilación y explotación de datos personales como necesario para el progreso social y tecnológico. Pero este modelo no ha valorado lo que supone en pérdida de nuestra privacidad. Y ello tiene un coste moral y político que no compensa los beneficios que genera. Solo si los datos personales son tratados con las debidas garantías y no como mera mercancía será posible un progreso auténtico hacia el bienestar sin la violación sistemática de los derechos individuales. La «privacidad», escribe la autora, «no debería ser el precio que tengamos que pagar para acceder a cualquiera de nuestros otros derechos, entre ellos la educación, la atención médica y la seguridad, primordial entre ellos» (Véliz, 2021, p. 208). Tenemos la responsabilidad de pensar en modelos que garanticen la seguridad y el bienestar sin vulnerar el derecho a la privacidad.

Pero la autora desconfía de dejar por completo tal tarea a la voluntad de los legisladores de reformar *motu proprio* el modelo de comercio de datos, la industria de la publicidad, el uso de datos sensibles, etc. En el trasfondo de su propuesta parece haber una concepción histórica y social de los derechos humanos, que solo son reconocidos, en palabras de Luigi Ferrajoli, tras luchas o revoluciones que han roto el velo de una precedente opresión o discriminación (Ferrajoli, 2011, p. 59). Pero solo llega a hacer explícita esta premisa al afirmar que «[l]a historia de los derechos es, en gran medida, la historia del reconocimiento progresivo de que los seres humanos no son recursos para explotar, sino individuos para respetar» (Véliz, 2021, p. 212). Esto es, los derechos no emergen sin más de su reconocimiento en documentos normativos, sino que son el resultado de demandas y presiones que empujan a la expansión de las fronteras del Derecho. Este evoluciona en la medida en que grupos e individuos, que no consideran suficientemente garantizada su dignidad en los derechos proclamados, contribuyen a generar una deliberación pública que aspira a desafiar, reinterpretar y transformar los derechos en un proceso social e institucional complejo. Como escribió Norberto Bobbio, los derechos «surgen gradualmente de las luchas que el hombre combate por su emancipación y de la transformación de las condiciones de vida que estas luchas producen» (Bobbio, 1991, p. 70). Esta concepción histórica y social de los derechos implica que son susceptibles de transformación y de ampliación. Lo que defiende Carissa Véliz es la necesidad de un compromiso individual y social con la transformación de la cultura imperante sobre la privacidad: escribir sobre ello, persuadir a otros de que protejan su privacidad, organizarse, desvelar el funcionamiento interno del sistema, demandar y apoyar alternativas privadas y públicas, concebir nuevas posibilidades y dejar de cooperar con un sistema injusto y opaco. Es necesario, en definitiva, disentir frente a lo inaceptable (Véliz, 2021, pp. 213, 240-242).

El ensayo se inserta en una cada vez más amplia literatura que pone ante nuestros ojos la improrrogabilidad de un análisis acerca de cómo es y cómo funciona el modelo digital-tecnológico que está determinando la estructura económica, cultural y política de nuestros días y cómo afecta a la privacidad. La autora se refiere particularmente a los trabajos de Bruce Schneier (2015, 2018), Cathy O'Neil (2016) y Yves-Alexandre de Montjoye (2013, 2015). Pero podrían sumarse otros muchos, como los ensayos de David Lyon (2007), Viktor Mayer-Schönberger y Kenneth Cukier (2013), Frank Pasquale (2015), o Marta Peirano (2019). Ahora conocemos más sobre

cómo se está explotando nuestra privacidad y existe mayor regulación acerca de la compilación y uso de nuestros datos. Por ello, según la autora, el momento actual es un momento histórico para sentar las bases de un modelo económico y social alternativo compatible con la privacidad.

1. El concepto de privacidad y los valores que lo respaldan

Pero ¿de qué hablamos cuando hablamos de privacidad? ¿y por qué debe importarnos? ¿qué la hace tan valiosa como para constituir una pretensión legítima de protección frente a otras pretensiones o intereses? Carissa Véliz no dedica un capítulo o epígrafe específico a contarnos a qué se refiere cuando habla de privacidad ni a qué la hace valiosa, a pesar de que estas han sido cuestiones disputadas habituales en las discusiones sobre privacidad sobre las que no ha habido nunca consenso (Thomson, 1975, p. 295). Sus presupuestos conceptuales y normativos se encuentran, sin embargo, más o menos implícitos a lo largo del texto.

Asumir el carácter histórico y dinámico del concepto de privacidad, al que me he referido, supone plantear qué sentido tiene en un contexto como el actual, que plantea retos y amenazas distintos de otros contextos sociales o culturales anteriores o diferentes. Los debates tradicionales sobre la privacidad, vinculados al pensamiento liberal, han girado en torno a la protección de intereses que solo conciernen al individuo frente a la interferencia de la sociedad y el poder público[1]. Esta dimensión individual de la privacidad ha abarcado muchas pretensiones normativas que podrían agruparse en torno a dos nociones: la de espacio y la de decisión. Por una parte, la idea de privacidad como espacio aislado y propio del individuo en el que el acceso es restringido se ha empleado para referirse a cuestiones relativamente separables como la soledad o reclusión, la inaccesibilidad, el anonimato, el secreto, la confidencialidad, la reserva, la confianza, la no vigilancia, el libre desarrollo de la personalidad o la diversidad de relaciones íntimas o privadas. Por otra parte, la privacidad se vincula a la idea de autonomía, de libertad para hacer elecciones sobre la vida propia y control sobre el modo de presentarnos ante los demás. Detrás de la idea de privacidad no hay una única pretensión que legítimamente se pretenda hacer valer bajo su amparo, sino un haz de exigencias normativas que giran en torno a la noción de libertad y capacidad del individuo de pensar, elegir y vivir.

En el libro *Privacy is Power* aparecen algunas de esas pretensiones que se entremezclan en la noción de privacidad. En algunas páginas aparece la idea de espacio libre de presiones externas, «una burbuja de protección de la sociedad» ajena a las miradas, juicios, preguntas e intrusiones de los demás. Este espacio permite «dejarse mutuamente ser» (*let one another be*) (Véliz, 2021, pp. 130, 249). Su relevancia exige que sea creada conscientemente para permitir que la creatividad y la libertad «pueden volar sin obstáculos» (Véliz, 2021, p. 218). En otras ocasiones, la privacidad se entiende en el libro como decisión, control, capacidad de mantener ciertos aspectos de nuestras vidas fuera del alcance de los demás: nuestros pensamientos, experiencias, conversaciones, planes; y libertad para decidir cómo vivir y con quien relacionarnos (Véliz, 2021, pp. 3, 84). «Privacidad y autonomía están relacionadas porque las pérdidas de privacidad facilitan que otros interfieran en tu vida» (Véliz, 2021, p. 84).

[1] El uso del propio término «privacidad» es novedoso en la literatura en castellano, tanto filosófica como política o jurídica, en la que ha sido habitual la traducción de *privacy* por intimidad. Esta es, quizá, la razón por la que ha sido más frecuente en esta literatura plantearse la «confusa relación entre intimidad y privacidad» (Toscano, 2017).

Hay una distinción importante para apreciar la complejidad de la idea de privacidad y que permite comprender en su radicalidad los atentados actuales contra ella, que no solo implican una vigilancia ubicua, sino que, además, se adentran en la configuración de nuestros deseos y preferencias. Esta irrupción afecta a lo que se considera el núcleo más profundo de la privacidad, constituido por lo que podemos denominar intimidad (Innes, 1992, p. 155). La distinción entre intimidad y privacidad, en el sentido de vida privada, aporta claridad conceptual y contribuye a analizar más precisamente los valores y riesgos que están detrás de las diversas dimensiones o ámbitos de la privacidad.

1.1. Lo íntimo y la vida privada

Lo íntimo, como expresó Ernesto Garzón Valdés en su artículo ya clásico, es «el ámbito de los pensamientos de cada cual, de la formación de decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será, no solo porque no se desea expresarlo, sino porque es inexpresable» (Garzón Valdés, 2003, p. 16). La reserva, la soledad o el anonimato nos liberan del condicionamiento de ser percibidos por otros y permite el libre desenvolvimiento de nuestros sentimientos, fantasías y pensamientos (Wasserstrom, 1984, p. 324; Nagel, 1998, p. 4). En las palabras tantas veces citadas de John Stuart Mill cuando se refiere a la libertad en relación con el «dominio interno de la conciencia» como la libertad de pensar y sentir, «la más absoluta libertad de pensamiento y sentimientos sobre todas las materias, prácticas o especulativas, científicas, morales o teológicas» (Mill, 1970, p. 68). Es en ese espacio íntimo, indecible e inaccesible, en el que el individuo se afirma en su singularidad, permitiendo que la particularidad no quede neutralizada bajo categorías que nos definen genéricamente. Así concebida, la intimidad desempeña algunas funciones esenciales, no solo para el libre desarrollo de la personalidad, sino también para la vida democrática: en primer lugar, el espacio íntimo libera de la tensión de estar sometidos a un orden colectivo y permite la reflexión individual crítica; en segundo lugar, hace posible la diversidad y pluralidad de pensamientos, ideas o creencias; y, en tercer lugar, la intimidad hace posible el ejercicio pleno de la autonomía desde la libertad de experimentar, fantasear o meditar sin rendir cuentas a los demás.

Las actuaciones íntimas «no pueden observarse y solo se las puede inferir a través de lo que el sujeto dice o hace, incluso con su inhibición o su silencio» (Castilla del Pino, 1989, p. 29). Por ello, lo que vulnera la intimidad es dar a conocer o atribuir intenciones o preferencias ocultas tras una actuación privada o pública de la que se pueden inferir. Es este uno de los modos en que las tecnologías digitales pueden llegar a afectar el núcleo más profundo de la privacidad, en cuanto que pueden identificar preferencias, orientaciones, dudas o creencias que el sujeto no ha dado a conocer conscientemente, reduciendo peligrosamente el reducto de lo íntimo. El riesgo de estas inferencias no es solo su carácter invasivo, sino también predictivo. En el primer caso, se vulnera el derecho de la persona a decidir cuándo y en qué contexto comunica o expresa los pensamientos, sentimientos y emociones, exteriorizando y exponiendo a abusos y manipulación aquello que el sujeto creía intrínsecamente inaccesible. La información personal se puede inferir sin que la haya proporcionado el propio sujeto (Véliz, 2021, pp. 36-37). Y esta es una de las bases del poder: la de, no solo actuar sobre los sujetos, sino construir sujetos. «El poder genera ciertas mentalidades, transforma sensibilidades, produce formas de ser en el mundo… Los deseos de las personas pueden ser en sí mismos el resultado del poder y, cuanto más invisibles son los medios de poder, más poderosos son» (Véliz, 2021, p. 61). Estas inferencias subrepticias desde marcadores involuntarios dejan completamente indefenso al sujeto ante resultados que pueden ser erróneos y conducir a decisiones injustas (Véliz, 2021, pp. 161-163).

En el segundo caso, se afecta gravemente la autonomía individual, al predecir una actuación futura antes de que la haya decidido el propio sujeto. Al aplicar los algoritmos predictivos a un perfil de sujeto se calcula la probabilidad de que ciertas personas compren ciertos productos, se comprometan políticamente con ciertos asuntos, incurran en ciertas acciones ilícitas, se relacionen con ciertas personas… y sobre esas predicciones se adoptan decisiones (Véliz, 2021, pp. 80, 244). Como afirma Ana Garriga, el perfil instaura ciertas formas de determinismo, al descubrir signos del que se prevé sea el comportamiento futuro (Garriga, 2015, pp. 69-70).

Resulta útil separar conceptualmente esta idea de intimidad, como lo que debería mantenerse en el interior de cada individuo, de la privacidad que se manifiesta y proyecta en decisiones y relaciones externas. Lo privado no es solo lo que permanece al interior del sujeto, sino lo que se hace y experimenta con «otros determinados». La vida privada es el espacio que compartimos con ciertas personas que queda confinado a terceros y en el que nos manifestamos del modo más parecido a lo que somos, donde expresamos y experimentamos nuestros deseos, miedos, aspiraciones, etc. La privacidad nos permite crear y mantener relaciones diversas y plurales, en contextos y con fines diversos. La capacidad de controlar cómo nos manifestamos y quién tiene acceso a nosotros nos permite mostrar diferentes facetas según las situaciones sociales y con quién estemos (Toscano, 2017, p. 545).

Lo que define la vida privada es el acceso restringido y el control sobre el modo en que nos manifestamos en las diversas relaciones. En este espacio de contacto con otros, pero separado de lo público, se realizan y llevan a cabo nuestros deseos y preferencias y se vive la vida propia conforme a lo que sentimos internamente. La interioridad se rebela de forma restringida y relativa en un contexto y para un fin concreto. Y cada contexto se rige por pautas propias que condicionan los roles, comportamientos, expectativas y tipo o cantidad de información que se comparte (Nissenbaum, 2010). La privacidad se aproxima a la intimidad tanto más cuanto estas relaciones están más orientadas y expresan especialmente sentimientos de afecto, amor o cuidado (Innes, 1992, p. 74). Pero la protección de las relaciones privadas no siempre se funda en que sean expresión de esa intimidad. También se protegen como privadas las relaciones en el ámbito de la salud, la educación, el empleo, la religión, o la economía y las finanzas, entre otras. Cada contexto tiene sus propios fines y valores, que determinan principios diversos de transmisión de información personal, tales como la confidencialidad, reciprocidad, consentimiento, merecimiento, obligación o necesidad.

Separar intimidad y vida privada es esencial para apreciar que el apego de la tradición liberal por atribuir una inmunidad no solo a la interioridad del individuo sino también a los espacios privados en que desarrolla su vida ha servido históricamente para ocultar desiguales condiciones individuales. La esfera privada siempre ha sido una esfera dominada por relaciones de poder. Su protección respecto de la intervención pública ha supuesto en muchos casos el silenciamiento del abuso y la opresión. No es solo la economía de datos, como asume Carissa Véliz, la que socava la igualdad individual (Véliz, 2021, pp. 100-101) ni la privacidad es la venda en los ojos del sistema que garantiza la imparcialidad (Véliz, 2021, p. 249). Una crítica a la economía digital conforme con las teorías críticas con la visión liberal del ámbito privado, construido sobre la ficción del sujeto abstracto soberano, no debe plantearse como forma de vigilancia y discriminación de una esfera que de otro modo sería autónoma e igualitaria. Del mismo modo que la economía de datos oculta la falta de soberanía de los usuarios del entorno digital, que están subordinados por su desigual capacidad de controlar acciones y decisiones respecto de quienes dominan el tratamiento de datos agregados, la esfera privada, en sus diversas dimensiones, oculta relaciones de dependencia que impiden también hablar de sujetos soberanos

y aislados (Weinberg, 2017). El ideal liberal de una vida privada, como desarrollo más adelante, no sirve para proteger a las personas de formas de dominación vinculadas a la privacidad. Como ha desarrollado la teoría feminista, cómo sea la esfera privada depende de condiciones impuestas en la esfera pública. La solución, por ello, solo puede ser política.

La tecnología ha transformado el modo en que lo privado en este segundo sentido se separa de lo público. La cultura digital descansa en gran medida en la publicidad de la vida privada, como modo de expresión y empoderamiento. Nuestra era digital ha aceptado la sobreexposición constante que ha sido calificada como «extimidad», no solo por el modo en que se acepta la proyección de nuestra interioridad, sino por cómo al hacerlo construimos nuestra propia forma de entendernos (Sibilia, 2009).

¿Significa esto el fin de la privacidad? Carissa Véliz se niega a aceptarlo y denuncia la asunción acrítica de que en la era digital la privacidad ha dejado de ser la norma social que rige la razonabilidad de los intercambios de información personal (Véliz, 2021, p. 50). Hemos asumido sin cuestionar un modelo cultural y económico que condiciona en gran medida la decisión de cada individuo acerca de lo que se reserva de su interioridad y lo que expone a los demás. «En la economía digital», escribe la autora, «todo el mundo se ve empujado a expresar más de lo necesario a los efectos de la amistad, la comunicación eficaz y el debate público, todo en un esfuerzo por crear más datos» (Véliz, 2021, p. 132). Y es tarea de todos, individual y colectivamente, restaurar una cultura de la privacidad, reaprender el valor de la privacidad para ser capaz de pensar libremente. Son nuestros valores los que deben orientar la innovación tecnológica. Nuestros datos no pueden servir solo para que las empresas ganen más dinero y nuestras instituciones acumulen poder sino para contribuir a la autonomía y el bienestar de las personas.

El denominado «capitalismo de la vigilancia» (Zuboff, 2019) se ha desarrollado sobre la materia prima de nuestras vidas, traducidas en datos. El verdadero negocio de las grandes empresas tecnológicas es la explotación económica de nuestros datos, a la que hemos contribuido con nuestra cooperación y asentimiento y que se ha consolidado con la colaboración de las instituciones públicas y privadas. Los gobiernos permitieron la recopilación indiscriminada de datos como fuente de poder que podrían utilizar para la garantía de la seguridad y los intereses del Estado. De esa colaboración ha surgido un modelo, no solo económico, sino social que ha transformado a los ciudadanos en usuarios y sujetos de datos (Véliz, 2021, pp. 3-5, 18, 32 y ss., 45, 241).

1.2. Protección de datos personales en el entorno digital

En el contexto de la «sociedad de la vigilancia» se producen cambios «cualitativos» en la concepción de la privacidad que no pueden obviarse. Carissa Véliz los tiene en cuenta, pero no marca suficientemente esta especificidad del problema de la privacidad en la era digital. Por una parte, la privacidad adquiere un sentido más objetivo que subjetivo, aludiendo a la «información» o «datos» personales que, en cuanto elementos materiales, están más expuestos a la difusión y la manipulación. En el subtítulo de su trabajo es donde la autora introduce este cambio en la idea de privacidad como control sobre los datos. Por otra parte, el entorno digital ha producido alteraciones tales en los procesos de recopilación, análisis y divulgación de datos que el interés legítimo en una expectativa razonable de privacidad se difumina peligrosamente.

La privacidad se traduce en datos cuando las experiencias humanas se recopilan, miden y analizan (Risse, 2019). La privacidad como protección de datos personales se refiere específicamente a la información personal que puede ser cuantificada y clasificada. Como se pregunta Véliz (2021, p. 32), ¿cómo acabaron nuestras experiencias de vida siendo datos? La respuesta nos remite al desarrollo y uso de tecnologías digitales que han traducido las cuestiones éticas implicadas en la idea de privacidad en un problema de control de datos.

Así concebida, la tutela de la privacidad se ha visto condicionada, especialmente en la cultura jurídica anglosajona, por una concepción iusprivatista para la que la libre circulación de los datos es un elemento esencial para la prestación de servicios y se debe dejar a la libre determinación de los sujetos. Se otorga preeminencia a las soluciones basadas en el mercado que, en la práctica, favorecen el uso libre de la información por el sector privado (Martínez, 2014a, pp. 3-4). Desde sus raíces liberales, el derecho a la privacidad se configura como un derecho sobre el que su titular puede disponer, análogo al derecho de propiedad. Véliz se une a quienes consideran improcedente esta analogía[2], refiriéndose especialmente a la interdependencia que nos hace vulnerables y responsables de la privacidad de los demás. «Nuestra interdependencia en materia de privacidad implica que ningún individuo tiene la autoridad moral para vender sus datos. No poseemos datos personales como poseemos una propiedad porque nuestros datos personales contienen los datos personales de otros. Tus datos personales no son solo tuyos» (Véliz, 2021, p. 93).

Además, en su libro asume las deficiencias del consentimiento y de la anonimización en el contexto de la economía de datos. Se ha escrito mucho, en primer lugar, sobre la dificultad de asegurar un consentimiento libre y específico del titular de los datos[3]. Como afirma Lorenzo Cotino, se ha acabado configurando como un simbolismo que «conlleva, a la postre, al fracaso de la privacidad pretendida y a la inoperancia del sistema de protección» (Cotino, 2017, p. 145). Carissa Véliz alude a la escasa predisposición de las grandes tecnológicas a pedirnos permiso para usar nuestros datos de forma indiscriminada y las estrategias para eludir la resistencia esperando que nos vayamos acostumbrando gradualmente a aceptar las condiciones que nunca habríamos aceptado si se nos hubieran presentado en un principio (Véliz, 2021, p. 157). Es el propio sistema en que opera el manejo de los datos, al que me referiré más abajo, el que está organizado de modo que resulta difícil que las personas adopten elecciones informadas y racionales.

En segundo lugar, tampoco existe un modo suficientemente satisfactorio de proteger la privacidad en el libre intercambio mediante la anonimización. Desafortunadamente, con demasiada frecuencia, es fácil re-identificar los datos anonimizados (Véliz, 2021, pp. 22-23, 155). Es posible que persistan datos que permitan esa identificación, o que sea posible la re-identificación mediante inferencias o por vinculación con otros paquetes de datos personales (Martínez, 2014b). Pero, incluso si se pudieran ampliar las garantías técnicas para el anonimato, las aplicaciones comunes de *big data* socavan los valores que el anonimato tradicionalmente ha protegido. Aunque los individuos no sean «identificables» pueden ser aún «accesibles», aún pueden estar representados de manera comprensible en registros que detallan sus atributos y actividades, y pueden estar sujetos a inferencias y predicciones adoptadas sobre esa base (Barocas y Nissenbaum, 2014, p. 45).

[2] Puede verse Véliz (Véliz, 2020). Se puede mencionar como muestra de esa literatura que recela del trato de los datos personales en términos propietarios los trabajos de Allen (1999) o Cohen (2000).
[3] Vid., por ejemplo, Oliver y Muñoz Soro (2013) o Solove (2013).

En un artículo clásico, Whitman contraponía la concepción iusprivatista de la privacidad a la concepción propia de la Europa continental que prima la idea de dignidad y respeto. En la concepción europea el florecimiento humano requiere la realización individual en formas que el mercado no puede proporcionar, primando la autodefinición sin restricciones a la soberanía del consumidor. La privacidad apela no tanto a un interés material cuanto a bienes inmateriales englobados en la idea amplia de la personalidad (Whitman, 2004, pp. 1181-1184, 1192-1194). Desde esta concepción, la mercantilización de la información personal debe verse restringida en aras de la protección del respeto y el reconocimiento recíprocos.

Esa concepción inmaterial del valor de la privacidad cobra, además, un sentido específico en el contexto de la era digital, en el que el desequilibrio entre el interés de empresas y gobiernos en la adquisición de datos y la capacidad de usarlos y el interés y posibilidades de los particulares es tal que convierte el problema de la privacidad en algo más amplio y complejo. Tanto Estados como corporaciones o particulares han usado siempre la tecnología más avanzada para vigilar y controlar, pero los métodos son cada vez más sofisticados y la digitalización ha supuesto un salto revolucionario.

Los motivos para considerarlo tal son diversos y en su mayoría van apareciendo de un modo u otro en el libro de Carissa Véliz. En primer lugar, por su extensión, esto es, el desmesurado aumento de los aspectos de nuestras vidas que la tecnología convierte en susceptibles de ser observados, recopilados y tratados. En segundo lugar, por las posibilidades de combinar o conectar múltiples datos (públicos y privados) que ofrecen información adicional de la que constituye cada uno de modo aislado. En tercer lugar, por las crecientes posibilidades técnicas para el almacenamiento, agregación, análisis, divulgación y aplicación de los datos que plantean cuestiones éticas y políticas que van más allá de la mera divulgación de lo que debería quedar oculto. En cuarto lugar, por la ruptura de los límites temporales y espaciales que hace cada vez más difícil diferenciar los momentos y espacios en los que se está actuando en lo privado. En su dimensión temporal, lo digital convierte lo privado en potencialmente disponible de modo indefinido, lo que supone, como afirma Véliz, perder la virtud de olvidar (Véliz, 2021, p. 172). En su dimensión espacial, las tecnologías de la comunicación hacen que la información se mueva por un territorio desespacializado (Thompson, 2011, p. 33).

En quinto lugar, por la opacidad acerca del modo en que son recopilados y tratados los datos y los fines a los que servirán. En sexto lugar, por la orientación de la recolección de datos a la categorización de las personas para generar perfiles psicológicos, esquemas de comportamiento o posibilidades de influencia que condicionarán las decisiones que se adopten respecto de ellas. Esta categorización genera desigualdad, produce pérdida de oportunidades, implica pérdida de autonomía y reduce la diversidad a modelos colectivos, lo que convierte el problema de la privacidad en otro distinto: no ya la identificabilidad de la interioridad de individuos sino la des-individuación (Turégano, 2020a, pp. 268-269). Los datos no logran capturar la complejidad de lo que somos, nuestra identidad dinámica y compleja tal y como la experimentamos. Nuestros datos no nos representan. La persona y el ciudadano se transforman en usuarios y sujetos de datos en la sociedad de la vigilancia (Véliz, 2021, pp. 4, 246). Por último, porque el *big data* se ha convertido en una parte inevitable de la vida personal y social. El entorno digital cumple en nuestros días funciones esenciales como repositorio de información, espacio para la socialización y la asociación política, lugar para la comunicación y el entretenimiento, foro para el comercio y las finanzas. Como tal, desempeña un papel central para el libre desarrollo de la personalidad, la formación y la investigación, la libertad de expresión y de asociación, la libertad política e ideológica y la libertad económica.

En esta situación a la que hemos llegado, la pérdida de privacidad supone un riesgo para otros valores con los que queda imbricada. Desatender la privacidad se ha entendido tradicionalmente como producción de daños a los intereses de un individuo. Y, en consecuencia, la garantía de la privacidad se ha concebido orientada al resarcimiento del individuo que sufre el daño. En un trabajo clásico William Prosser identificaba cuatro tipos de daño que habían venido siendo protegidos por los tribunales del *common law* en el ámbito del *tort law*: intrusión en la soledad o reclusión de una persona, revelación pública de hechos privados incómodos sobre una persona, información que ofrece una imagen distorsionada de alguien ante el público y apropiación de la apariencia de uno en provecho de otro (Prosser, 1960). Pero en la actualidad, los riesgos son más amplios y elevados que en el mundo pre-internet (Véliz, 2021, p. 138). El sistema generado por las tecnologías digitales no solo agudiza el riesgo de estos daños individuales, sino que daña a la sociedad en su conjunto, afectando a cuestiones de seguridad, igualdad y justicia. En gran medida, la protección de datos personales es importante en nuestros días porque implica la protección de esos otros valores. La definición de la privacidad, «durante largo tiempo únicamente conexa al «derecho de ser dejado solo», se dilata y dirige hacia la idea de tutela global de las opciones de vida contra toda forma de control público y de estigmatización social» (Rodotà, 2003, p. 21).

Son diversos los valores que están en riesgo cuando la privacidad queda desatendida (Turégano, 2020b, pp. 30-37). Un argumento habitual en contra de una protección amplia de la privacidad es el riesgo que implica a la «seguridad». Sin embargo, en la literatura reciente es habitual la idea de que es la pérdida de la privacidad lo que implica inseguridad, derivada fundamentalmente del modo en que la información se obtiene y gestiona y la incapacidad de los sujetos de conocer y participar en los procesos de recolección y análisis de la información personal. En segundo lugar, el modelo vigente de tratamiento de datos no garantiza la imparcialidad de los criterios para la inclusión o exclusión de ciertas informaciones o servicios ni transparencia en los principios que determinan la generación de perfiles y la categorización, produciendo «discriminación». El flujo de información produce, en tercer lugar, «injusticia» cuando traspasa el contexto y fines para los que fue recabada. Se trata de un problema de relevancia: cualquier selección o aplicación de datos personales debería limitarse a un propósito o necesidad funcional legítimo. Es una cuestión, en quinto lugar, de «respeto» y «reconocimiento» que exige que los individuos no sean tratados como objetos de los que se extrae información sin ninguna opción real de reciprocidad ni de participación. Por último, ese «olvido del reconocimiento» (Honneth, 2007) es consecuencia de la «mercantilización» de los datos que, igual que fenómenos como la industria del sexo o la gestación subrogada, han naturalizado el trato al otro como objeto. La lógica económica sustituye a la lógica comunicativa, afectando a elementos esenciales de la integración social (Roessler, 2015, pp. 152-155).

La conclusión a la que llegamos desde estas premisas es una de las ideas centrales del libro: el sacrificio de la privacidad no es una renuncia ineludible en la era digital, sino una restricción injustificable de un «derecho» humano básico que tenemos el deber de evitar. Los datos personales son un producto tóxico, susceptible de abuso y difícil de mantener seguro. Como tal, no deberían ser compilados y tratados sin restricciones. La economía de datos ha supuesto un modelo de desarrollo basado en gran medida en una explotación de esos datos que afecta al libre desarrollo de la personalidad y genera desigualdad e injusticia. Debemos trabajar en común para pensar e instituir otro desarrollo posible.

2. La dimensión social de la privacidad

La privacidad es mucho más que un interés individual de reserva y aislamiento. Hay un valor en vivir en una sociedad que respeta la privacidad (Solove, 2015). No se trata solo de mejorar las vidas de los individuos, sino de construir sociedades más justas e igualitarias. El derecho a la privacidad puede compararse con otros derechos, como el derecho a la ciencia o la libertad de expresión, en los que el interés individual en la investigación o en comunicar las ideas puede también mostrarse como un interés social en una comunidad científica o en una oferta diversa y plural de ideas (Vayena y Tasioulas, 2016, p. 8; Regan, 1995, p. 214). Es un error suponer, escribe Véliz, que porque tratemos con datos personales, la privacidad sea un asunto personal (Véliz, 2019).

Desde los años setenta ha habido una interesante literatura que ha subrayado la dimensión social de la privacidad (Turégano, 2020b). Se ha resaltado el aspecto relacional del valor de la privacidad, que permite configurar socialmente espacios diversos para relaciones íntimas, familiares, laborales, sanitarias, educativas o financieras, entre otras muchas (Rachels, 1975; Nissenbaum, 2010). Esta perspectiva relacional se vincula a una concepción del individuo como sujeto situado y socialmente construido y de la personalidad como un complejo de dimensiones y facetas que se expresan y desarrollan en contextos diversos. Así concebida, la privacidad no apela solo a la seclusión o a la desvinculación de la vida social sino a la capacidad de expresarse y ser en una variedad de asociaciones (Schoeman, 1992). De modo que la revelación de la intimidad es el resultado de la elección del individuo de buscar y participar en la interacción social (Steeves, 2009, p. 199).

Esta dimensión social de la privacidad está muy presente en el libro de Carissa Véliz. Son principalmente tres las ideas que están detrás de su tesis de que la «privacidad es colectiva». En primer lugar, la privacidad de cada uno se entremezcla con la de los demás. Esta interconexión nos hace vulnerables unos a otros y nos convierte en responsables de la privacidad de los demás (Véliz, 2021, p. 93). De este carácter colectivo del valor de la privacidad deriva que no puede ser facilitado ni protegido de modo individual. La privacidad es un bien público porque no puede ser proporcionado, manejado ni protegido de forma privada en el complejo contexto institucional comunicativo existente (Regan, 2015, pp. 62-65). Proteger la privacidad es un problema de acción colectiva: de modo análogo al cambio climático, un acto individual no produce el desastre, pero sí la suma de ellos con el paso del tiempo y las consecuencias son sufridas por todos (Véliz, 2021, pp. 219, 88-89). En un entorno digital, la determinación de los estándares de privacidad y el control del flujo de información es demasiado complejo para que cada usuario lo administre por sí mismo. El diseño de la regulación de la privacidad debe hacerse desde propósitos y objetivos colectivos.

En segundo lugar, Véliz sostiene que las consecuencias de la erosión de la privacidad no solo son personales sino también colectivas. Los ciberataques y el robo de datos no solo ponen en riesgo a personas concretas, sino que permiten reclutar colaboradores, ensayar algoritmos, acceder a información de relevancia pública, identificar la localización de personal militar o instalaciones estratégicas o colapsar servicios básicos poniendo en riesgo la seguridad nacional (Véliz, 2021, pp. 115-119, 167-171). Un entorno digital inseguro es extremadamente peligroso para individuos, compañías y sociedades. Pero invertir en ciberseguridad no es rentable para las empresas tecnológicas. Solo mediante la intervención pública puede garantizarse la seguridad. El uso de datos es igual que la producción y uso de edificios, medicamentos, productos alimenticios, automóviles o aviones en la común necesidad de estándares públicos. A pesar de sus reticencias iniciales, empresas y sociedades

aceptan la regulación que les protege a ellas y a sus clientes de los desastres de seguridad. «Y llegan a darse cuenta de que la regulación es a veces la única forma en que una empresa puede invertir en algo valioso que no tiene un rendimiento inmediato sin incurrir en una desventaja competitiva, porque todos los demás también tienen que hacerlo» (Véliz, 2021, p. 168).

En tercer lugar, la privacidad no solo es valiosa para nuestra vida personal sino también para nuestra vida como ciudadanos. Una cultura de la privacidad favorece que seamos sinceros, audaces y originales, tengamos conversaciones íntimas y debates francos en un entorno seguro, estableciendo los vínculos en los que se basan las sociedades liberales. Una sociedad de la vigilancia solo alimenta conformidad y silencio y desincentiva la crítica y la controversia (Véliz, 2019; 2021, p. 94). Lo privado no solo es necesario para el desarrollo de la persona, sino también para producir una esfera pública abierta y plural. Para organizarnos social y políticamente, para formar y formular ideas y juicios propios y disentir de las dominantes necesitamos un espacio libre y común.

La esfera digital ha aspirado a convertirse en la extensión de la esfera pública, suministrando información, proporcionando el espacio para la socialización, lugar para la comunicación que incorpora voces y problemas diversos y proporcionando el espacio para el intercambio y la discusión. Sin embargo, como afirma Marta Peirano, hemos cometido dos errores: pensar que las redes sociales eran un espacio de debate público imparcial y pedirles que tomaran decisiones que las empresas no deberían tomar. Su objetivo no era convertirse en la nueva ágora sino un modelo de negocio vinculado a mantenernos conectados para recopilar masivamente nuestros datos y venderlos con fines publicitarios (Peirano, 2019). Esta economía de la atención, como la ha denominado James Williams (2021), nos distrae de las conversaciones importantes sobre justicia, economía, ecología o bienes públicos (Véliz, 2021, p. 132).

La realidad de la esfera pública digital es la de un público categorizado, fragmentado y mediatizado por corporaciones privadas con pocas posibilidades para el debate abierto y plural. En la esfera digital cada uno accede a contenidos e informaciones acordes con sus intereses y preferencias, en un fenómeno que se ha calificado como «cámaras eco» (Sunstein, 2003) o «filtros burbuja» (Pariser, 2017). Se priorizan ciertos asuntos sobre otros, radicalizando el debate al sobredimensionar ideas marginales y reforzar prejuicios (Marantz, 2021). Se da prioridad a la emotividad y la indignación sobre los debates constructivos (García Merino, 2020). Y el rechazo y hostilidad en las redes acaba produciendo autocensura (York y Zuckerman, 2019), reduciendo la pluralidad y dificultando el intercambio y la interacción constructiva. Las potencialidades de una esfera pública digital incluyente pueden llegar a ser reales si se dan ciertas precondiciones. La privacidad es una de esas precondiciones necesarias: es necesaria para divulgar información acorde con nuestras creencias y sin presión, protestar anónimamente sin temor a represalias, asociarse libremente, leer sobre lo que tenemos curiosidad (Véliz, 2021, p. 96).

La privacidad es un valor instrumental para el disfrute efectivo de derechos básicos para la democracia, tales como la libertad de asociación y reunión, la libertad de expresión, la libertad ideológica, la libertad de manifestación y la libertad de voto. Los Estados que quieran garantizar realmente las libertades políticas e ideológicas deben comprometerse con la protección de la privacidad (Nyst, 2013). La eliminación de la privacidad mediante el procesamiento ilimitado de datos personales podría terminar reemplazando la democracia por un gobierno algorítmico en el que los ciudadanos perderían poder de decisión. La vieja política ideologizada, subjetivista y arbitraria se considera superable por una acción de gobierno más racional y apolítica

que hará posible el conocimiento objetivo e irrefutable que proporciona el tratamiento tecnológico de los datos (Innerarity, 2021).

La realidad es que el análisis de datos genera nuevas relaciones de poder. El manejo de las grandes cantidades de datos requiere el empleo de algoritmos automatizados para detectar patrones y tomar decisiones. El acceso, control y uso de la tecnología necesaria está desigualmente distribuido, lo que intensifica las asimetrías de poder entre quienes tienen la capacidad de recopilar y analizar los datos y quienes simplemente los alimentan (Innerarity, 2021). Hace ya años autores como Vittorio Frosini (1982) o Antonio Enrique Pérez Luño (1992) escribieron sobre la libertad informática como libertad positiva de ejercer el control sobre los datos personales, pudiendo conocer, corregir, eliminar o añadir datos de archivos electrónicos, frente a los agentes privados y públicos que detentan el «poder» informático.

Pero, además, la recopilación, análisis y uso de los datos se produce en el marco de un sistema complejo en el que interactúan elementos técnicos, prácticas culturales y sociales, estructuras organizativas, actores sociales y significados. La tecnología se fusiona con el entorno formando el «mundo de la vida digital» que impregna nuestra experiencia y se integra en todas las estructuras y objetos (Susskind, 2018, p. 42). Véliz asume esta idea del mundo digital como sistema o estructura, al considerar el modelo de economía de datos como un modelo que depende de la vulneración «sistemática» de derechos (2021, p. 208) y hablar de un «ecosistema de datos» (2021, p. 210). El sistema opera bajo la creencia en el poder y validez de los patrones extraídos de conjuntos de datos masivos para hacer predicciones y adoptar decisiones sin necesidad de juicios o valoraciones políticas. Pero los resultados no son neutros ni objetivos, en la medida en que dependen del diseño e instrucciones que se inserten en el código. Si nuestra reflexión ética se dirige a esa infraestructura sociotécnica, de prácticas, actitudes, reglas y expectativas, no puede ser solo una reflexión sobre la conducta moral de los agentes implicados sino, además, una reflexión sobre la «infraestructura ética» o «infraética», en palabras de Luciano Floridi (2017); es decir, una reflexión sobre cómo esa infraestructura puede facilitar y promover buenas decisiones y acciones.

Quienes controlan esos sistemas ejercen poder en la medida en que tienen capacidad para condicionar las actuaciones de otros[4]. Se trata de un tipo particular de poder que consiste en la capacidad de acumular, procesar y aplicar datos personales no solo para condicionar la conducta de otros sino para influir en la construcción de su propia subjetividad. Como afirma Véliz, este poder es el tipo de poder por antonomasia de la era digital. Pero no se trata solo, como afirma la autora, de un poder derivado del conocimiento de detalles personales (2021, pp. 60-62), sino algo mucho más complejo, a lo que alude en diversos momentos de su trabajo. Es un poder que controla la infraestructura y el proceso que hace que nuestros datos sean recopilados y usados de un modo opaco e indeterminado. La metáfora que expresa esta situación no es tanto la que se emplea habitualmente del «Gran Hermano» orweliano o el «Panóptico» foucaultiano, cuanto la imagen de «El Proceso» de Franz Kafka y su descripción del sentimiento de indefensión y vulnerabilidad que se experimenta cuando una organización o estructura controla nuestras vidas sin que sepamos qué ocurre o podamos defendernos frente a ella (Solove, 2001). El problema no es que se conozcan aspectos íntimos de las personas, sino que ese conocimiento

[4] Véliz (2021, p. 58) emplea una definición de poder de Rainer Forst muy similar a las de Max Weber (1964), que lo definía como probabilidad de imponer la propia voluntad en una relación social o la de Robert Dahl (1957), para quien alguien tiene poder sobre otro en la medida en que puede conseguir que haga algo que de otro modo no haría.

se construye y codifica en un entramado institucional difícilmente accesible y que no se orienta a que el individuo realice sus propias metas y deseos.

La mayor arbitrariedad de este poder es la imposibilidad de conocer las razones y valores que subyacen a las operaciones que realiza. El ecosistema sociotécnico ha progresado sin haberse producido el necesario debate social (Schwarz, 1999, p. 1612). Y lo que está en juego no es solo la protección de la individualidad, sino la cuestión de los desequilibrios de poder en nuestras sociedades. Pero no son solo los datos en sí los que empoderan, sino la estructura sistémica de recopilación y explotación de esos datos. Dejarla operar con una lógica propia al margen de las voluntades democráticas supone una dejación irresponsable y peligrosa.

La privacidad importa porque hace que el poder lo tengan los ciudadanos, que es a quienes corresponde en una democracia (Véliz, 2021, p. 96). Y, según la autora, hemos cedido gran parte de nuestro poder en un momento en que la democracia está débil (Véliz, 2021, pp. 97, 248). Anne Applebaum, la autora que nos habla en su reciente ensayo sobre el creciente auge y asedio que sufren las democracias occidentales por las ideas antiliberales y las élites autoritarias, denuncia cómo estas utilizan la polarización y la transición a la esfera digital para cambiar nuestra vida política (García Merino, 2020). No podemos renunciar a nuestra privacidad y facilitar mucha información sin conocer y participar en las diversas fases del tratamiento automatizado de nuestros datos. El ensayo de Véliz nos conduce a reflexionar acerca de cómo ha de ser ese proceso. Jamie Susskind señala tres posibles modos de hablar de legitimidad en este contexto: como consenso, si se puede suponer que los sujetos han consentido efectivamente a verse sometidos al poder de la estructura sociotécnica; como reciprocidad, en cuanto que quienes aceptan sus beneficios tienen el deber de aceptar sus cargas; o como expresión de valores comunes, si se entiende que el ejercicio del poder refleja o encarna los valores compartidos. Mientras el sistema sea poco transparente y opaco y los agentes públicos y privados que participan en el mismo mantengan sus algoritmos ocultos, sus políticas de datos oscuras y sus fines y valores indefinidos, no podrán reclamar ninguna de estas formas de legitimidad (Susskind, 2018, pp. 351-355).

3. Here´s how[5]

Privacy is Power no solo nos muestra qué lejos estamos de un sistema digital aceptable en términos de privacidad, sino que la autora quiere movernos a la acción. El libro cierra con un capítulo titulado «Lo que puedes hacer» en el que nos ofrece consejos prácticos para recuperar el control sobre nuestros datos, como cambiar *Google* por motores de búsqueda amigables con la privacidad como *DuckDuckGo*, crear espacios de privacidad pidiendo a nuestros invitados no tomar fotos o videos o no publicarlos *on line*, pedir permiso a las personas antes de publicar información que les atañe o avisarles de los dispositivos que tenemos, usar extensiones y herramientas de privacidad o elegir dispositivos «tontos» en lugar de «inteligentes». En definitiva, anima a rechazar lo inaceptable, a disentir cuando sea necesario. «Depende de nosotros motivar a las empresas y los gobiernos para proteger nuestra privacidad. Podemos hacer que suceda. Y para que nuestra cultura comience a preocuparse por la privacidad nuevamente, no es necesario que alcances la perfección: hacer lo mejor que puedas es suficiente» (Véliz, 2021, p. 240).

Coherentemente con su concepción de la privacidad como un asunto colectivo y político, Véliz no solo incentiva a la acción particular sino a la acción política y la

[5] Con esta expresión termina la autora su Introducción al libro (2021, p. 6).

intervención jurídica. Es cierto, sin embargo, que en ocasiones la autora deja traslucir cierta desconfianza hacia el compromiso del legislador. No solo porque sus propuestas al mismo las deja en un capítulo anterior al capítulo de cierre en el que llama a la acción particular, sino también porque desconfía de que el legislador vaya a asumir algunas de las recomendaciones que le hace. Por ejemplo, al terminar su argumentación en favor de la prohibición de anuncios personalizados concluye que «"[a]fortunadamente", no tienes que esperar a que los legisladores reformen la industria de la publicidad: puedes usar bloqueadores de anuncios» (Véliz, 2021, p. 152). Igualmente, tampoco tienes que esperar a que el legislador prohíba el comercio de datos personales para empezar a trabajar para ese objetivo (Véliz, 2021, p. 156).

Aunque la implicación de la ciudadanía y el empoderamiento de los individuos es esencial para cambiar el modelo existente, el carácter sistémico de la vulneración de la privacidad y el carácter social de los valores y las consecuencias implicadas obligan a una apuesta más contundente con un enfoque político-jurídico. La contribución del Derecho es esencial para asegurar las restricciones y garantías en el proceso de recopilación y uso de los datos personales, sobre la base de un principio básico de minimización de datos, recogido en el artículo 5 del Reglamento Europeo de Protección de Datos, conforme al cual los datos empleados solo han de ser aquellos adecuados, pertinentes y limitados a lo necesario en relación con los fines a los que se orienta su tratamiento. Es necesario reflexionar acerca del modo en que se puedan formalizar y adaptar las exigencias del debido proceso al tratamiento de datos, de modo que los individuos y sus datos sean tratados de acuerdo con reglas predeterminadas y comprensibles. Los sistemas de adopción de decisiones automatizadas han de rendir cuentas y cumplir estándares básicos de justicia. Los individuos deben tener garantizado el modo de impugnar decisiones adversas basadas en categorizaciones incorrectas (Barocas y Selbst, 2016; Citron y Pasquale, 2014; Kroll et al., 2017; Balkin, 2017). En sentido similar, la implantación de un «*Habeas Data*» supone garantías procesales para hacer efectiva la facultad del individuo de conocer y controlar las informaciones que le conciernen procesadas en bancos de datos. La privacidad, desde esta perspectiva, no es solo capacidad de autodeterminación del individuo, sino también de co-determinación o participación activa en los procedimientos que le afecten (Pérez Luño, 1992). Carissa Véliz en este libro solo deja planteadas estas exigencias. Escribe que la recopilación y el análisis de datos no deben realizarse sin garantía jurídica y solo deben ocurrir si es necesario. También deben ser específicos (en contraposición a la vigilancia masiva) y proporcionales a las circunstancias (Véliz, 2021, pp. 181-182).

Quienes operan en el ecosistema de datos tienen una responsabilidad especial en el uso ético de los mismos debido al enorme poder que les confiere la ingente cantidad de datos que manejan, el control que ejercen sobre las herramientas tecnológicas que se emplean para recopilarlos y tratarlos, los enormes beneficios que ello les reporta y los deberes que tienen respecto de la sociedad en general por la función que desempeñan. Carissa Véliz expresa esta idea con el concepto de deberes fiduciarios de las entidades, públicas y privadas, que manejan datos personales. Estos deberes existen para proteger a individuos que están en una posición de debilidad o vulnerabilidad frente a profesionales que se supone que han de servirles pero que pueden tener intereses en conflicto y con los que existe una asimetría de poder y conocimiento (Véliz, 2021, p. 164). La responsabilidad de cada agente depende de la posición que ocupa en la estructura: su posición de poder o influencia, la situación de privilegio o beneficio respecto del proceso, el interés en la superación

de la injusticia y la capacidad de cambiar la estructura que produce injusticia (Turégano, 2020a, p. 277)[6].

Nos enfrentamos, pues, a cuatro grandes desafíos: más educación y concienciación a la ciudadanía; más regulación que establezca restricciones y garantías; más transparencia en el proceso de quién y para qué se usan nuestros datos y evaluación de su impacto en la privacidad; y más inversión en innovación en privacidad: fomentar medidas preventivas de privacidad desde el diseño y por defecto.

Quiero terminar con el dilema que planteaba al comienzo. Nuestros datos pueden ser usados maliciosamente en contra de nuestros intereses o de los intereses generales. Pero la información que proporcionamos de modo más o menos voluntario también puede ser socialmente útil. Una regulación demasiado garantista de la privacidad podría ser un impedimento para asegurar bienes comunes como la salud, la seguridad, la planificación urbana, más eficientes sistemas de transporte o energía, la investigación, o el patrimonio de la Hacienda Pública, en el ejemplo con el que comenzaba. ¿Hasta qué punto no debemos ceder nuestros datos por el bien común? En un momento determinado, Carissa Véliz escribe que «[p]rohibir el comercio de datos personales no significa prohibir la recopilación o el uso adecuado de dichos datos» (Véliz, 2021, p. 155). Un poco antes afirma que lo que debe evitarse es que el poder que se acumula a través de los datos se transforme en poder económico o poder político. «Los datos personales deberían beneficiar a los ciudadanos» (Véliz, 2021, p. 154). Parece, pues, que la protección no debe ser tanto de los datos personales en sí sino del uso inadecuado o desviado de los mismos.

Sin embargo, la premisa de la que la autora parte al plantear la cuestión de la privacidad y el bien común es su concepción de los datos personales como producto sensible y vulnerable que, aún con una finalidad pública justificada, debe ser manejado con las máximas garantías y cautelas. En relación con los datos médicos, a los que dedica un apartado específico, niega la premisa mayor: que el avance de la medicina solo pueda lograrse mediante el uso de datos personales. Ello por tres razones: primero, por su escepticismo ante el poder de la tecnología digital, que ha hecho promesas excesivas y ha tenido un rendimiento inferior al esperado; segundo, por la existencia de modos de usar datos personales que minimicen el riesgo de los pacientes y les compensen; y, tercero, por la posibilidad de avances médicos importantes que podrían no requerir datos (Véliz, 2021, pp. 195-202). ¿Supone esta respuesta que deben evitarse en la medida de lo posible los avances en la promoción de bienes públicos que solo pueden lograrse con el uso de datos personales identificables? ¿el uso de datos personales con fines públicos supone siempre una violación de la privacidad?

El alegato de la autora en favor de estar alerta para que los periodos de crisis no se aprovechen para que el control que se ha cedido transitoriamente sobre derechos no se recupere cuando pase la tormenta, parece asumir que la privacidad es un valor absoluto que se garantiza o al que se renuncia (Véliz, 2021, pp. 202-209). Ella misma nos ha dicho que los datos personales tienen un valor colectivo, que constituyen un recurso común de utilidad general. Esto implica que la pretensión legítima del individuo de control sobre su vida privada no tiene carácter absoluto, sino que entra en juego con otros intereses comunes legítimos sobre los datos personales.

[6] Véliz se refiere a la responsabilidad en función de la contribución de cada individuo a la estructura institucional. «Las empresas y los gobiernos están formados por individuos y, aunque algunos individuos tienen más poder que otros para dirigir una institución en una dirección u otra, cada individuo es moralmente responsable de todo lo que contribuya a esa institución» (2021, p. 237).

En este sentido, la dicotomía entre privacidad y bienes comunes plantea un problema de coordinación de dos intereses «sociales» (Solove, 2015, p. 80).

Pero esa coordinación puede interpretarse de modos distintos. Se puede plantear el dilema entre privacidad y bienes comunes, como la salud, bien en términos de proporcionalidad entre derechos en conflicto, o bien en términos de la necesaria determinación o redefinición del contenido de la privacidad en contextos cambiantes. El esquema de la proporcionalidad analiza los criterios para determinar razonablemente en qué casos está justificada la restricción de la privacidad. Debe existir una amenaza cierta y de gran alcance a un interés social legítimo, la idoneidad y necesidad de una medida restrictiva de la privacidad para salvaguardarlo y la exigencia de la mínima intrusión posible. La determinación del tercer criterio –qué resulta menos intrusivo– depende de la consideración de tres dimensiones: el nivel de sensibilidad de la información, el volumen de información recopilada y el alcance de la digitalización, procesamiento y distribución de los datos (Etzioni, 2015, pp. 6-12).

Pero no es necesario presentar la relación entre privacidad y los bienes públicos a los que puede servir el *big data* como un conflicto sistémico resoluble solo de modo particularizado. El derecho a la privacidad tiene un carácter dinámico, cambiando su alcance en función de los cambios que se producen en el contexto en que rige. De modo que, aunque aceptemos que existe un interés legítimo en desarrollar nuestra personalidad y ejercer un control razonable sobre el modo en que nos presentamos a los demás, determinar qué deberes corresponden a ese derecho es una cuestión compleja, que debe ser especificada a la luz de otros intereses y de su factibilidad en circunstancias cambiantes. No se trata de ponderar en cada caso posible de conflicto, sino de determinar los deberes que implica cada derecho de modo que puedan ser satisfechos generalmente de modo conjunto. Ello supone un enfoque holístico en la determinación del contenido de la privacidad que tiene en cuenta cómo interactúa con un entorno cambiante y con otros derechos y fines legítimos (Vayena y Tasioulas, 2016).

Los cambios que suponen las circunstancias de las sociedades digitales pueden suponer un cambio en el contenido de la privacidad, ajustándolo a las posibilidades y exigencias de un contexto diferente. Lo que pensamos y sentimos acerca de la privacidad no es estático. No solo han cambiado los intereses protegidos por el Derecho, en cuanto que han cambiado los daños derivados de la pérdida de privacidad. También han cambiado los deberes correlativos, que pueden orientarse no tanto a la poco factible exigencia de que el titular tenga un control exclusivo sobre el flujo de datos, cuanto al establecimiento de condiciones bajo las que son permisibles ciertos usos de datos, orientados a fines legítimos. Por ejemplo, en relación con la investigación médica basada en datos, la privacidad puede requerir que los beneficios sean compartidos de modo justo entre la comunidad; que los usuarios de datos no los sometan a búsquedas que creen ciertos riesgos, y si tales riesgos surgen, que la información recopilada no sea divulgada a nadie que pueda usarla para dañar a la persona en cuestión; que los usuarios de datos se comprometan a una completa transparencia sobre el uso de datos y las acciones relacionadas; que los tratamientos discriminatorios sean castigados y compensados por ley; o que se ofrezcan opciones a los individuos una vez que hayan sido adecuadamente informados (Vayena y Tasioulas, 2016, pp. 11-12).

La digitalización ha alterado profundamente nuestro mundo y ha traído consigo desafíos nuevos o de distinta escala. Algunas de las más recientes propuestas políticas europeas en materia antiterrorista o de *copyright* marcan una cierta línea hacia la relajación en la protección de la privacidad. El reciente Reglamento (UE)

2021/1232 del Parlamento Europeo y del Consejo de 14 de julio de 2021, por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea está marcando el debate estos días. La norma obedece al peligroso aumento que el uso de las tecnologías ha favorecido del abuso sexual en línea. El Reglamento legaliza la colaboración voluntaria −que habría quedado prohibida por el Código Europeo de Comunicaciones Electrónicas de diciembre de 2020− que los proveedores de servicios de correo electrónico, chat y mensajería prestan en la detección del abuso, mediante tecnología *hashing* y datos de tráfico, y lo denuncien. En su intento por compatibilizar el control con la privacidad, el artículo 3 del Reglamento establece que las tecnologías utilizadas deben ser las menos intrusivas para la intimidad a la vista del estado de la técnica en el sector. El Reglamento delimita temporal y materialmente el alcance de la excepción y reconoce el derecho a la tutela judicial efectiva de los usuarios que consideren que sus derechos han sido vulnerados como consecuencia del tratamiento de datos. La propuesta normativa de la Unión Europea, en donde rigen altos estándares jurídicos de protección de la privacidad, ha levantado enormes suspicacias entre activistas, políticos y expertos en privacidad. El debate está abierto y no ha hecho más que comenzar. Es el momento de deliberar de modo abierto acerca de qué sociedad digital queremos. El procedimiento, las garantías y las responsabilidades correlativas a la privacidad deberían consensuarse en un nuevo «*Data Deal*»[7] que afiance el equilibrio entre quienes proporcionan información de sus vidas y quienes se benefician de ello.

Bibliografía

Allen, A. L. (1999). Coercing Privacy. *William & Mary Law Review*, *volumen 40*(3), pp. 723-757.

Balkin, J. M. (2017). The Three Laws of Robotics in the Age of Big Data. *Ohio State Law Journal*, *78*, pp. 1217-1241.

Barocas, S. y Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. En J. Lane, V. Stodden, S. Bender y H. Nissenbaum (eds.), *Privacy, Big Data, and the Public Good* (pp. 44-75). Nueva York, Estados Unidos: Cambridge University Press.

Barocas, S. y Selbst, A.D. (2016). Big Data's Disparate Impact. *California Law Review*, *104*, pp. 671-732

Bobbio, N. (1991). Presente y porvenir de los derechos humanos, en *El tiempo de los derechos*. Madrid, España: Sistema.

Castilla del Pino, C. (1989). Público, privado, íntimo. En C. Castilla del Pino (ed.), *De la intimidad* (pp. 25-31). Barcelona, España: Crítica.

Citron, D. y Pasquale, F. (2014). The Scored Society, Due Process for Automated Predictions. *Washington Law Review*, *89*, pp. 1-33.

Cohen, J. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, *52*, pp. 1373-1437.

Cotino, L. (2017). Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Dilemata*, *24*, pp. 131-150.

Dahl, R. (1957), The Concept of Power. *Behavioral Science*, *2*(3), pp. 201-215

De Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. y Blondel, V.D. (2013). Unique in the Crowd: The Privacy Bounds of Human Mobility. *Scientific Reports, 3*(3), p. 1376.

[7] Emplea esta expresión Susskind (2018, pp. 336-340).

De Montjoye, Y.-A., Radaelli, L., Singh, V. K. y Pentland, A. S. (2015). Identity and privacy. Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. *Science*, *347*(6221), pp. 536-539.

Domínguez Cebrián, B. (7 de julio, 2021). El manejo de los datos será en el futuro una amenaza a la seguridad nacional. *El País*. https://elpais.com/internacional/2021-07-07/el-manejo-de-los-datos-sera-en-el-futuro-una-amenaza-a-la-seguridad-nacional.html#:~:text=Janis%20Sarts%3A%20%E2%80%9CEl%20manejo%20de,nacional%E2%80%9D%20%7C%20Internacional%20%7C%20EL%20PA%C3%8DS

Etzioni, A. (2015*). Privacy in a Cyber Age. Policy and Practice*. Nueva York, Estados Unidos: Palgrave Macmillan.

Ferrajoli, L. (2011). *Principia Iuris. Teoría del Derecho y de la Democracia*, volumen II, p. 59. Madrid, España: Trotta.

Floridi, L. (2017). Infraethics. On the Conditions of Possibility of Morality. *Philosophy and Technology*, *30*(4), pp. 391-394.

Frosini, V. (1982). *Cibernética, Derecho y sociedad*. Madrid, España: Tecnos.

García Merino, L. (23 de diciembre, 2020). Anne Applebaum: "Es necesario mantener un debate distinto sobre cómo funciona internet y las redes sociales y cuál es su relación con la política. *Foro Telos, Fundación Telefónica*. Recuperado de https://telos.fundaciontelefonica.com/foro-telos-2020-anne-applebaum-es-necesario-mantener-un-debate-distinto-sobre-como-funciona-internet-y-las-redes-sociales-y-cual-es-su-relacion-con-la-politica/

Garriga, A. (2015). *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua*. Madrid, España: Dykinson.

Garzón Valdés, E. (2003). Lo íntimo, lo privado y lo público. *Claves de Razón Práctica*, 137, pp. 14-24.

González, R. (12 de julio, 2021). El Big Data sigue la pista a los ricos que dicen vivir falsamente en el extranjero. *Big Data Magazine*. Recuperado de https://bigdatamagazine.es/el-big-data-sigue-la-pista-a-los-ricos-que-dicen-vivir-falsamente-en-el-extranjero

Honneth, A. (2007). *Reificación. Un estudio en la teoría del reconocimiento*. Buenos Aires, Argentina: Katz.

Innerarity, D. (18 de abril, 2021). Grandes datos, pequeña política. *El País*. https://elpais.com/ideas/2021-04-17/grandes-datos-pequena-politica.html

Innes, J.C. (1992). *Privacy, Intimacy and Isolation*. Nueva York, Estados Unidos: Oxford University Press.

Kroll, J. et al. (2017). Accountable Algorithms. *University of Pennsylvania Law Review*, *165*, pp. 633-705.

Lyon, D. (2007). *Surveillance Studies. An Overview*. Cambridge, Reino Unido: Polity Press.

Marantz, A. (2021). *Antisocial. La extrema derecha y la libertad de expresión en Internet*. Madrid, España: Capitán Swing.

Martínez, R. (2014a). Privacidad, EE.UU y España. Tan lejos tan cerca. *Telos. Cuadernos de Comunicación e innovación*, *97*, pp. 1-9.

Martínez, R. (2014b). Ética y privacidad de los datos. *Ponencia presentada en Big Data: de la investigación científica a la gestión empresarial, Fundación Ramón Areces*. Recuperado de http://sgfm.elcorteingles.es/SGFM/FRA/recursos/conferencias/ppt/1776180509_1472014102438.docx (última consulta el 23/07/21).

Mayer-Schönberger, V. y Cukier, K. (2013). *Big Data. A Revolution that Will Transform How We Live, Work, and Think*. Nueva York, Estados Unidos: Houghton Mifflin Harcourt. Edición castellana Mayer-Schönberger, V. y Cukier, K. (2013). *Big data. La revolución de los datos masivos*. Madrid, España: Turner Publicaciones.

Mill, J.S. (1970). *Sobre la libertad*. Madrid, España: Alianza.

Nagel, T. (1998). Concealment and Exposure. *Philosophy & Public Affairs*, *27*(1), pp. 3-30.
Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford, Estados Unidos: Stanford University Press.
Nyst, C. (2013). El derecho a la privacidad y a la libertad de expresión: dos caras de la misma moneda. *Cuestión de derechos*, *4*, pp. 24-32.
O'Neil, C. (2016). *Weapons of Math Destruction*. Nueva York, Estados Unidos: Crown. Edición castellana O'Neil, C. (2017). *Armas de destrucción matemática*. Madrid, España: Capitán Swing.
Oliver A. D. y Muñoz Soro, J.F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En J. Valero Torrijos, *La protección de los datos personales en Internet ante la innovación tecnológica* (pp.153-196). Cizur Menor, España: Aranzadi.
Pariser, E. (2017). *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos*. Madrid, España: Taurus.
Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, Estados Unidos: Harvard University Press.
Peirano, M. (2019). *El enemigo conoce el sistema. Manipulación de ideas, personas e influencias después de la economía de la atención*. Barcelona, España: Debate.
Pérez Luño, A.E. (1992). Intimidad y protección de datos personales: del *Habeas Corpus* al *Habeas Data*. En L García San Miguel (ed.), *Estudios sobre el derecho a la intimidad* (pp. 36-45). Madrid, España: Tecnos.
Prosser, W. (1960). Privacy. *California Law Review*, *48*, pp. 383-423.
Rachels, J. (1975). Why Privacy is Important?. *Philosophy & Public Affairs*, *4*(4), pp. 323-333.
Regan, P. (1995). *Legislating privacy: Technology, social values and public policy*. Chapel Hill, Estados Unidos: The University of North Carolina Press.
Regan, P. (2015). Privacy and the Common Good: Revisited. En B. Roessler y D. Mokrosinska (eds.), *Social Dimensions of Privacy. Interdisciplinary Perspectives* (pp. 50-70). Cambridge, Reino Unido: Cambridge University Press.
Risse, V. (2019). Private Data and Property. En IE University, *Data, Privacy, and the Individual. Madrid: Center for the Governance of Change*. Recuperado de www.ie.edu/cgc/research/data-privacy-individual (última consulta 23/07/21)
Rodotà, S. (2003). Democracia y protección de datos. *Cuadernos de Derecho Público,* 19-20, pp. 15-26.
Roessler, B. (2015). Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy. En B. Roessler y D. Mokrosinska (eds.), *Social Dimensions of Privacy. Interdisciplinary Perspectives* (pp. 141-161). Cambridge, Reino Unido: Cambridge University Press.
Schneier, B. (2015). *Data and Goliath*. Londres, Reino Unido: W. W. Norton & Company.
Schneiner, B. (2018). *Click Here to Kill Everybody. Security and Survival in a Hyper-Connected World*. Nueva York, Estados Unidos: W. W. Norton & Company. Edición castellana Schneiner, B. (2019). *Haz clic aquí para matarlos a todos. Un manual de supervivencia*. Barcelona, España: Temas de Hoy-Planeta.
Schoeman, F. (1992). *Privacy and Social Freedom*. Cambridge, Reino Unido: Cambridge University Press.
Schwartz, P.M. (1999). Privacy and Democracy in Cyberspace. *Vanderbilt Law Review*, *52*, pp. 1609-1701.
Sibilia, P. (2009). *La intimidad como espectáculo*. Buenos Aires, Argentina: Fondo de Cultura Económica.
Solove, D.J. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, *53*, pp. 1393-1462.
Solove, D.J. (2013). La autogestión de la privacidad y el dilema del consentimiento. *Revista Chilena de Derecho y Tecnología*, *2*(2), pp. 11-47.

Solove, D.J. (2015). The Meaning and Value of Privacy. En B. Roessler y D. Mokrosinska (eds.), *Social Dimensions of Privacy. Interdisciplinary Perspectives* (pp. 71-81). Cambridge, Reino Unido: Cambridge University Press.
Steeves, V. (2009). Reclaiming the Social Value of Privacy. En I. Kerr, V. Steeves y C. Lucock (eds.), *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society* (pp. 191-208). Nueva York, Estados Unidos: Oxford University Press.
Sunstein, C.R. (2003). *República.com. Internet, democracia y libertad*. Madrid, España: Paidós.
Susskind, J. (2018). *Future Politics. Living together in a World Transformed by Tech*. Oxford, Reino Unido: Oxford University Press.
Thomson, J.J. (1975). The Right to Privacy. *Philosophy & Public Affairs*, *4*(4), pp. 295-314.
Thompson, J. B. (2011). Los límites cambiantes de la vida pública y privada. *Nueva Época*, 15, enero-junio, pp. 11-42.
Toscano, M. (2017). Sobre el concepto de privacidad: la relación entre privacidad e intimidad. *Isegoría. Revista de Filosofía Moral y Política*, *57*, pp. 533-552.
Turégano Mansilla, I. (2020a). Los valores detrás de la privacidad. *Doxa. Cuadernos de Filosofía del Derecho*, *43*, pp. 255-283.
Turégano Mansilla, I. (2020b). La dimensión social de la privacidad en un entorno virtual. En O. Fuentes Soriano (dir.), *Era digital, sociedad y Derecho* (pp. 27-54). Valencia, España: Tirant lo Blanch.
Vayena, E. y Tasioulas, J. (2016). The dynamics of big data and human rights: the case of scientific research. *Philosophical Transactions of the Royal Society*, pp. 1-14.
Véliz, C. (22 de octubre, 2019). Privacy is a Collective Concern. *NewStatesman*. https://www.newstatesman.com/science-tech/privacy/2019/10/privacy-collective-concern
Véliz, C. (2020). Private Data and Property. En IE University, Center for the Governance of Change, *Data, Privacy and the Individual. Privacy Matters*, p. 9.
Véliz, C. (2021). *Privacy is Power. Why and How You Should Take Back Control of Your Data*. Londres, Reino Unido: Bantam Press.
Wasserstrom, R.A. (1984). Privacy: Some arguments and assumptions. En F. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 317-332). Cambridge, Reino Unido: Cambridge University Press.
Weber, M. (1964). *Economía y sociedad*. Ciudad de México, México: Fondo de Cultura Económica.
Weinberg, L. (2017). Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden. *Westminster Papers in Communication and Culture*, *12*(3), pp. 5-20.
Whitman, J.Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, *113*(6), pp. 1151-1222.
Williams, J. (2021). *Clics contra la humanidad. Libertad y resistencia en la era de la distracción tecnológica*. Barcelona, España: Gatopardo Ediciones.
York, J.C. y Zuckerman, E. (2019). Moderating the Public Sphere. En Jørgensen, R.F. (ed.), *Human Rights in the Age of Platforms* (pp. 137-161). Cambridge y Londres, Reino Unido: The MIT Press.
Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. Londres, Reino Unido: Profile Books. Edición castellana Zuboff, S. (2020). *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*. Barcelona, España: Paidós.