



LA PRIVACIDAD
COMO INSTRUMENTO
DE RESISTENCIA
COLECTIVA

CARISSA VÉLIZ

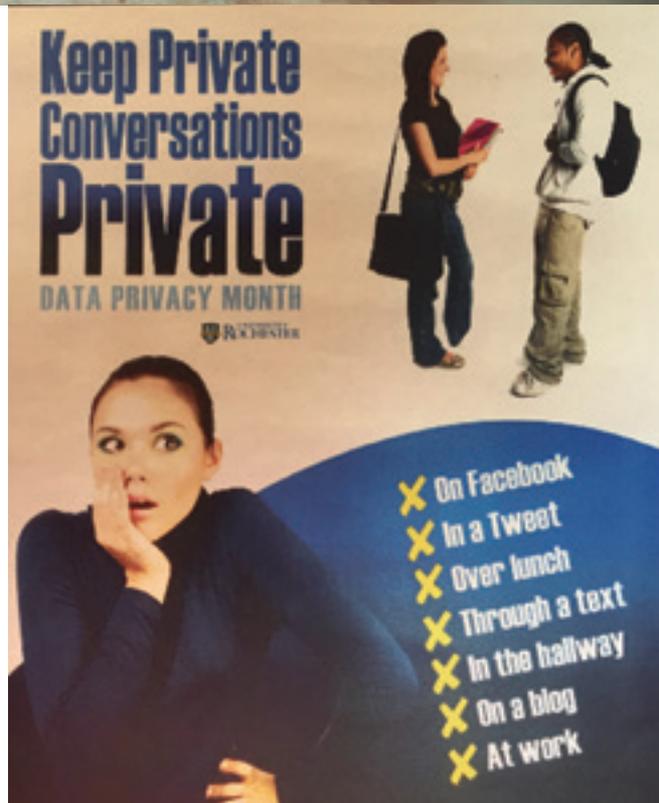
Profesora en el Institute for Ethics in AI,
Oxford University

*Una versión más completa de este artículo se puede encontrar en Carissa Véliz, *Privacy Is Power* (Bantam Press 2020), traducido en español como *Privacidad es poder* (Debate, 2021).

El punto de partida de este texto es invitar al lector a imaginar que dispone de una llave maestra, única y especial, que da acceso a los ámbitos más íntimos de su casa: a su dormitorio, sus armarios, su archivo, su diario personal, sus datos médicos, a la correspondencia o los mensajes que ha intercambiado. ¿Sería razonable sacar infinitas copias de esa misma llave y regalársela a todo aquel que nos cruzáramos por la calle —o, aún peor— ¿a todo aquel transeúnte que mostrase un alto interés por usarla en nuestra ausencia? Muy probablemente, la respuesta sería no, ya que sería solo cuestión de tiempo que alguien abusase de nuestra ingenuidad. Entonces, ¿cómo se explica nuestra cándida disposición a regalar nuestros datos personales a todo aquel que nos los pide?

La tesis de este texto es que nuestra privacidad actúa en cierto modo como la citada llave, ya que protege los aspectos más íntimos y personales de los individuos, los que los singularizan, y también los que los hacen más vulnerables. La privacidad nos sirve para cobijar nuestras fragilidades y nuestras pasiones, fantasías, miedos y también aquellos recuerdos que preferiríamos olvidar. Salvaguarda el mapa de los resortes, conscientes e inconscientes, que mueven nuestras acciones, pasiones y emociones.

Al entregarle esa llave —la privacidad— a un ser querido, generamos cercanía con esa persona, quien, de manera cómplice, usará la llave para ayudarnos, orientarnos y aumentar nuestro bienestar. Parte de lo que significa la cercanía emocional con alguien es compartir lo que nos hace vulnerables; revelar nuestro talón de Aquiles y confiar en que el otro no aprovechará dicha ventaja para herirnos o sacar provecho. Las personas que nos quieren bien pueden usar nuestra fecha de nacimiento para organizarnos una fiesta de cumpleaños sorpresa; anotarán nuestros gustos y tendrán presentes nuestros miedos más oscuros para mantenernos a salvo. Sin embargo, no todos usarán el acceso privilegiado a nuestra vida personal para favorecernos: los estafadores pueden usar esos mismos datos para suplantar nuestra identidad y cometer un delito; las empresas pueden usar nuestros gustos para atraernos a un mal negocio; nuestros enemigos pueden usar nuestros miedos para amenazarnos y extorsionarnos. La privacidad es importante porque nos hace más libres; cuando se desvanece, otros pueden ganar poder sobre nosotros.



Google y Facebook no están realmente en el negocio de los datos; están en el negocio del poder que les confieren los datos

Solo soy una persona más... ¿Quién puede interesarse en mí y qué tenemos todos que perder?

Podríamos pensar que como personas comunes y corrientes no tenemos nada que ocultar, nada que temer. Este postulado es erróneo, a menos que uno desee exponerse a la suplantación de identidad, discriminación, desempleo, humillación pública y al riesgo del totalitarismo, entre otras desgracias. Planteemos pues la tesis a la inversa; si esta información no fuera relevante (y reveladora) las empresas y los gobiernos no dedicarían tantos esfuerzos y recursos de todo tipo al desarrollo de tecnologías invasivas y de control masivo de los datos.

Como individuos, un capital del que disponemos aún es el de la presencia mental —el objeto en el que fijamos nuestra atención. Sin embargo, existe una pugna creciente por atraerla a todo tipo de medios y aplicaciones —que monetizan el tiempo y la audiencia— y con ello, cuantificar esa atención y presentarla como ganancia. Las empresas quieren saberlo todo sobre ti para saber cómo distraerte, aunque ello signifique que pases menos tiempo con tus seres queridos, o que no atiendas a necesidades básicas como el sueño.

Los proveedores de contenidos (que hoy incluyen a las empresas audiovisuales, pero también a los *influencers* individuales o a los *youtubers*) pugnan por tener el máximo número de suscriptores. Los *hackers* ansían obtener información o imágenes sensibles con las que llevar a cabo extorsiones y secuestros de identidades digitales y de servidores en red. Las compañías de seguros también anhelan ganar nuevos

clientes, siempre y cuando estos presenten un riesgo mínimo, en una evaluación que es mucho más efectiva si disponen de datos personales, en particular los relativos a la salud. También las empresas desean tener acceso a información reservada de sus potenciales nuevos trabajadores, como por ejemplo su implicación en la defensa de los derechos laborales.

Pero la ambición de traspasar el muro de la privacidad tiene impactos que van más allá del individuo singular. Todos tenemos contactos personales. Somos un nodo en una red de relaciones humanas: somos la hija/o de unos padres, el vecino de una vecina, el maestro, la abogada o el barbero de otros. A través de cada uno de los nodos, pueden llegar a todos los integrantes de la red. Ese es el motivo de que las aplicaciones soliciten el acceso a los contactos. También tenemos una voz, un perfil en redes sociales que todo tipo de agentes querrían poder controlar para convertirnos en portavoces de sus objetivos y de su visión del mundo, en los medios sociales y más allá. También disponemos de un voto; agentes extranjeros y nacionales pugnan por poder interferir y aumentar los apoyos al candidato que mejor defienda sus intereses. Aun tomados individualmente, somos personas muy importantes. Somos fuentes de poder.

La naturaleza del poder

A estas alturas, la mayoría de las personas son conscientes de que sus datos valen dinero. Pero estos datos no son valiosos exclusivamente porque pueden ser comercializados. Técnicamente, Facebook no vende los datos

de sus usuarios. Tampoco Google. Lo que venden es el poder de influenciar en las decisiones de sus usuarios. Ven den el poder de mostrarte anuncios y el poder de predecir tu comportamiento. Google y Facebook no están realmente en el negocio de los datos; están en el negocio del poder que les confieren los datos. Más que un beneficio económico, los datos personales otorgan poder a quienes los recogen y los analizan, y eso es lo que los hace tan codiciados.

Este poder tiene dos vertientes. La primera es la que el filósofo alemán Rainer Forst ha definido como “la capacidad de A para motivar a B a pensar o hacer algo que de otro modo B no habría pensado o hecho”¹. Los medios a través de los cuales los poderosos ejercen su influencia son diversos. Abarcan desde los discursos motivadores, las recomendaciones, las visiones ideológicas del mundo, la seducción y la presentación de amenazas creíbles. Forst argumenta que la fuerza bruta o la violencia no es un ejercicio de poder, pues las personas sometidas no “hacen” nada, sino que es a ellas a quienes se les hace algo. Pero claramente la fuerza bruta sí es un ejemplo de poder. Es contraintuitivo pensar que alguien que nos tiene sometidos mediante la violencia carece de poder. Es el caso, por ejemplo, de un ejército que oprime a la ciudadanía, o el de un grupo mafioso o criminal que aterroriza a una comunidad. En *Economía y Sociedad* (1978), el economista político alemán Max Weber describe este segundo aspecto del poder como la capacidad de las personas y las instituciones para “llevar a cabo su propia voluntad a pesar de la resistencia”².

En resumen, las personas e instituciones poderosas nos inducen a actuar y pensar en formas en las que no actuaríamos y pensaríamos si no fuera por su influencia. Y si con eso no es suficiente, pueden ejercer la fuerza sobre nosotros —y hacernos lo que nosotros mismos no haríamos.

Hay diferentes tipos de poder: económico, político, militar, etc. El poder es como la energía: puede tomar muchas formas diferentes, y estas pueden transformarse. Una empresa rica a menudo puede utilizar su dinero para influir en la política a través del cabildeo (*lobbying*), por ejemplo, o puede influir en la opinión pública a través del uso de la publicidad.

1. Véase Forst, 2015.
2. Véase Weber, 1978.

El que gigantes de la tecnología como Facebook y Google sean poderosos no sorprende a nadie. Sin embargo, una exploración más profunda de la relación entre privacidad y poder debería permitirnos una mejor comprensión de cómo las instituciones acumulan, ejercen y transforman el poder en la era digital, lo que a su vez puede darnos herramientas e ideas para la resistencia frente a este tipo de dominación, que resulta de las violaciones de nuestro derecho a la privacidad.

Sobre la relación entre poder, conocimiento y privacidad

Hay una estrecha conexión entre el conocimiento y el poder. El primero es, como mínimo, un instrumento de poder. El filósofo francés Michel Foucault va aún más allá y argumenta que el conocimiento es en sí mismo una forma de poder³. Hay poder en el conocer. Al proteger nuestra privacidad, evitamos que otros puedan tener un conocimiento sobre nosotros que pueda ser utilizado en contra de nuestros intereses.

Cuanto más sepa alguien sobre nosotros, más podrá anticiparse a cada uno de nuestros movimientos e influirnos. Una de las contribuciones más importantes de Foucault a nuestra comprensión del poder es la idea de que este no solo *actúa* sobre los seres humanos, sino que *construye* sujetos humanos (lo que no impide que podamos resistirnos al poder y luchar por construirnos a nosotros mismos). El poder genera ciertas mentalidades, transforma las sensibilidades, trae consigo formas de estar en el mundo. En ese sentido, el teórico político británico Steven Lukes argumentó en su libro *Power* (1974) que el poder puede alumbrar en las personas deseos que van en contra de sus propios intereses⁴. Y cuanto más invisibles sean los medios del poder, más poderosos serán. Por ejemplo, el poder crea preferencias cuando usa lo que sabemos sobre el sistema de la dopamina para diseñar aplicaciones adictivas, o cuando se personalizan los anuncios políticos en base a información personal (como hizo Cambridge Analytica en varias campañas electorales en EEUU, en Argentina, o el referéndum del Brexit).

El poder que surge como resultado del conocimiento de los datos personales de un individuo es un tipo de poder muy particular. Al igual que el poder económico y el político, el que da la privacidad permite a quienes lo detentan la posibilidad de transformarlo en otros tipos de poder. Es, además, la quintaesencia del poder en la era digital.

En el año 2000, dos años después de su creación y pese a su gran popularidad, Google todavía no había desarrollado un modelo de negocio sostenible y diferencial del resto de *startups*. Todo cambió con el lanzamiento de AdWords (actualmente Google Ads), que dio el pistoletazo de salida a la explotación económica de los datos producidos por las interacciones de los usuarios, en este caso de Google, con el objetivo de vender anuncios. En menos de cuatro años, la compañía logró un aumento del 3.590% en sus ingresos⁵.

Ese mismo año, la Comisión Federal de Comercio había recomendado al Congreso de los Estados Unidos que se regulara la privacidad en línea. Sin embargo, tras los atentados del 11 de septiembre de 2001 contra las Torres Gemelas de Nueva York, la preocupación por la seguridad primó sobre la privacidad, y se abandonaron los planes de regulación. La economía digital pudo despegar y alcanzar la magnitud de la que goza hoy en día porque los gobiernos tenían interés en tener acceso a los datos de la gente. Desde el principio, la vigilancia digital se ha mantenido gracias a un esfuerzo conjunto de instituciones públicas y privadas.



Tener el poder de conocer la resistencia organizada antes de que esta se manifieste, y ser capaz de aplastarla a tiempo, es el sueño de cualquier tirano

3. Véase Dreyfus y Rabinow, 1982.

4. Véase Lukes, 2005.

5. Véase Zuboff, 2019.



La recopilación y el análisis masivo de datos personales han dotado de nuevos poderes tanto a los gobiernos como a las empresas que espían. Los gobiernos saben, ahora más que nunca, las interioridades de los ciudadanos. La Stasi (el servicio de seguridad de la República Democrática Alemana), por ejemplo, solo consiguió tener archivos de un tercio de la población, aunque aspiraba a tener información completa sobre todos los ciudadanos. Las agencias de inteligencia tienen hoy en día mucha más información sobre toda la población. Una proporción significativa de personas ofrece voluntariamente información privada en las redes sociales. Como dijo la cineasta estadounidense Laura Poitras en una entrevista con *The Washington Post* en 2014, “Facebook es un regalo para las agencias de inteligencia”⁶. Entre otras posibilidades, este tipo de información da a los gobiernos la capacidad de anticiparse a las protestas, e incluso de arrestar preventivamente a las personas que planean participar en ellas. Tener el poder de conocer la resistencia organizada antes de que esta se manifieste, y ser capaz de aplastarla a tiempo, es el sueño de cualquier tirano.

6. Véase Peterson, 2014.

El poder de las empresas tecnológicas está constituido, por un lado, por el control exclusivo de los datos y, por otro, por la capacidad de anticiparse a cada uno de nuestros movimientos, lo que a su vez les da la oportunidad de influir en nuestro comportamiento y vender esa influencia a otros. Las empresas que obtienen la mayor parte de sus ingresos a través de la publicidad han utilizado nuestros datos como una ventaja competitiva que ha hecho imposible que las empresas alternativas desafíen a los titanes de la tecnología. El motor de búsqueda de Google, por ejemplo, es tan efectivo en parte porque su algoritmo tiene muchos más datos de los que aprender que de los que disponen cualquiera de sus competidores. Con la cantidad de datos a los que tiene acceso, Google puede saber qué es lo que te mantiene despierto por la noche, qué es lo que más deseas y qué planeas hacer mañana. La empresa susurra esta información a otros entrometidos que quieren mostrarte anuncios personalizados.

Las empresas también pueden compartir nuestros datos con “agentes de datos” (*data brokers*) que crearán un archivo sobre nosotros basándose en todo lo que ya saben (o, mejor dicho, en todo lo que creen saber), y luego lo venderán a quienes estén dispuestos a comprarlo: aseguradoras, gobiernos, posibles empleadores e incluso estafadores.

Los “buitres de datos” son increíblemente inteligentes en el uso de los dos aspectos del poder discutidos anteriormente: nos hacen renunciar a nuestros datos, de forma más o menos voluntaria, y también nos los arrebatan, incluso cuando intentamos resistirnos. Las tarjetas de fidelización son un ejemplo de poder que nos lleva a hacer ciertas cosas que de otra manera no haríamos. Cuando te ofrecen un descuento por fidelidad en tu supermercado local, lo que te ofrecen es que esa compañía te vigile y luego influya en tu comportamiento a través de empujones o *nudges* (descuentos que te animarán a comprar ciertos productos). Un ejemplo de cómo el poder actúa en contra de nuestra voluntad se da cuando Google graba nuestra ubicación en un teléfono Android, incluso cuando le hemos dicho que no lo haga⁷.

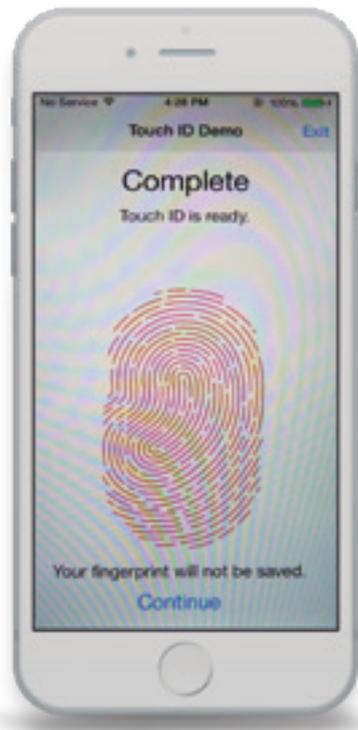
Ambos tipos de poder también operan a un nivel más general en la era digital. La tecnología nos seduce constantemente para que hagamos cosas que de otra manera no haríamos, desde perdernos en una cola de reproducción de vídeos en *YouTube*, hasta jugar a juegos sin sentido, o revisar nuestro teléfono cientos de veces al día. La era digital ha traído nuevas formas de estar en el mundo que no siempre mejoran nuestras vidas. De forma más subrepticia, la economía de datos también ha logrado normalizar ciertas formas de pensar. Las compañías tecnológicas quieren que pensemos que, si no hemos hecho nada malo, no tenemos ninguna razón para oponernos a que almacenen nuestros datos. También quieren que pensemos que tratar tus datos como una mercancía es necesario para la tecnología digital, y que la tecnología digital es progreso, incluso cuando parece más un retroceso social o político. Y lo que es más importante, los mercaderes tecnológicos quieren que pensemos que las innovaciones que sacan al mercado son inevitables. Son progreso, y el progreso no se puede detener.

Ese relato es complaciente y engañoso. Como señala el geógrafo económico danés Bent Flyvbjerg en *Rationality and Power: Democracy in Practice* (1998), el poder produce el conocimiento, las narrativas y la racionalidad que conducen a construir la realidad que ansía⁸. Pero una tecnología que perpetúa las tendencias sexistas y racistas

7. Véase Associated Press, 2018.

8. Véase Flyvbjerg, 1998.

9. Véase Véliz, 2019a.



y que agrava la desigualdad no constituye ningún progreso⁹. Las invenciones están lejos de ser inevitables. Tratar los datos como una mercancía es una forma de que las empresas ganen dinero, y no tiene nada que ver con la creación de buenos productos. Acumular datos es una forma de acumular poder. En lugar de preocuparse solo por ganar tanto dinero como sea posible, las empresas de tecnología pueden y deben preocuparse por diseñar el mundo en línea de manera que contribuya al bienestar de las personas. Tenemos muchas razones para oponernos a que las instituciones recopilen y utilicen nuestros datos de la manera en que lo hacen.

Una de esas razones es que con ello las instituciones atropellan nuestra autonomía, nuestro derecho al autogobierno. Aquí es donde la vertiente más dura del poder entra en juego. Hasta ahora, la era digital se ha caracterizado en que las instituciones hagan lo que quieran con nuestros datos, pasándose por alto y sin escrúpulos nuestro consentimiento cuando creen que el objetivo lo merece. En el mundo analógico, ese tipo de comportamiento se describiría como “robo” o “coerción”. El hecho de que no se llame por su nombre en el mundo digital es otra prueba del poder de la tecnología sobre las narrativas dominantes.

¿Existe margen para la resistencia?

Afortunadamente, no todo son malas noticias. Ciertamente, las instituciones en la era digital han acumulado mucho poder mediante el abuso de nuestra privacidad, pero podemos reclamar los datos que almacenan y limitar la recolección de nuevos datos. En términos de Foucault, aún tenemos la posibilidad de resistir al poder y construirnos a nosotros mismos. El poder de las grandes tecnológicas parece muy sólido. Pero el castillo de naipes está construido en parte sobre mentiras y sustracciones. Es posible ponerle fin a la economía de datos. Los poderes de la tecnología no son nada sin nuestros datos. Un pequeño esfuerzo de regulación, un poco de resistencia de los ciudadanos, y unas pocas empresas que empiecen a ofrecer privacidad como una ventaja competitiva, y todo podría evaporarse.

Las propias empresas de tecnología son más conscientes que nadie de su vulnerabilidad. Es por eso que están tratando de convencernos de que les importa nuestra privacidad después de todo (a pesar de lo que sus abogados digan en los juzgados). Por eso gastan millones de dólares en *lobbying*. Si estuvieran tan seguros del valor de sus productos para el bien de los usuarios y de la sociedad, no tendrían que presionar tanto a los gobiernos. Las empresas de tecnología han abusado de su poder, y es hora de resistirse.

En la era digital, la resistencia al abuso de poder ha sido calificada de *techlash* (reacción negativa frente a la tecnología). La historia nos recuerda que el poder debe conocer límites y contrapesos para que sea una influencia positiva en la sociedad. Incluso un entusiasta acérrimo de la tecnología, convencido de que no hay nada malo en lo que las empresas de tecnología y los gobiernos hacen con nuestros datos, debería querer ponerle límites al poder, ya que nunca se sabe quién será el próximo en ostentarlo. La evidencia dicta que las empresas de tecnología han ayudado a los regímenes totalitarios en el pasado, y no existe una distinción clara entre la vigilancia gubernamental y la corporativa. Las empresas comparten datos con los gobiernos, y las instituciones públicas comparten datos con las empresas. Este ha sido un punto especialmente controvertido durante la pandemia global de coronavirus, durante la cual algunos estados han facilitado enormes volúmenes de datos personales —y sanitarios— de sus ciudadanos a grandes corporaciones privadas (como Palantir).

Debemos exigirnos, por lo menos, oponer resistencia a la economía de datos. Abstenerse de usar la tecnología por completo es poco realista para la mayoría de las personas, pero existen multitud de opciones intermedias. Por ejemplo, respetar la privacidad de los demás y no exponer a otros ciudadanos a través de Internet. No fotografiar a personas sin su consentimiento, y no compartir imágenes en las que estas aparezcan. Minimizar la cantidad de datos que se entregan a instituciones que no tienen derecho a reclamarlos. Como señalan los expertos en medios de comunicación Finn Brunton y Helen Nissenbaum¹⁰, existe también la opción de la ofuscación. Si una compañía de ropa nos pide el nombre para vendernos ropa, damos un nombre diferente —por ejemplo, Dr. Información Privada, para que reciban el mensaje. No les demos a estas instituciones pretextos que sugieran que estamos de acuerdo en que se lleven nuestros datos. Dejemos claro que no lo consentimos libremente.

Cuando descargemos aplicaciones y compremos productos, elijamos aquellos productos que favorezcan la privacidad. Usemos extensiones de privacidad en los navegadores. Desactivemos los servicios de Wi-Fi, Bluetooth y localización del teléfono cuando no los necesitamos. Usemos las herramientas legales a nuestra disposición para pedir a las empresas los datos que tienen sobre nosotros, y también pidámosles que los eliminen. Cambiemos nuestra configuración para proteger la privacidad. Abstengámonos de usar uno de esos kits de pruebas de ADN en casa —no valen la pena. Olvidémonos de los timbres “inteligentes” que violan nuestra privacidad y la de los demás. Escribamos a nuestros representantes políticos compartiendo nuestras preocupaciones sobre la privacidad. Tuiteemos sobre ello. Aprovechemos las oportunidades que se nos presenten para informar a las empresas, los gobiernos y otras personas que nos preocupa la privacidad, que lo que se están haciendo con nuestros datos no está bien.

No cometamos el error de pensar que estamos a salvo de los daños que pueden ocurrir a raíz de una pérdida de privacidad. Tal vez seas joven y tengas salud. Podrías pensar que tus datos solo pueden ir a tu favor y

nunca en tu contra, si has tenido suerte hasta ahora. Pero es posible que tu salud falle, y no serás joven para siempre. La democracia que das por sentada podría convertirse en un régimen autoritario que actúe en tu contra.

Además, nuestra privacidad no es algo que nos atañe solo a nosotros. La privacidad es tanto personal como colectiva¹¹. Cuando exponemos nuestra privacidad, nos ponemos a todos en riesgo. La privacidad es necesaria para la democracia, para que la gente vote de acuerdo con sus creencias y sin presiones indebidas, para que los ciudadanos protesten anónimamente sin miedo a las repercusiones, para que los individuos tengan libertad para asociarse, decir lo que piensan, leer sobre lo que despierta su curiosidad. Si vamos a vivir en una democracia, el grueso del poder debe estar con la ciudadanía. Si la mayor parte del poder reside en las empresas, tendremos una plutocracia. Si la mayor parte del poder reside en el Estado, tendremos algún tipo de autoritarismo. La democracia no es algo dado, sino algo por lo que tenemos que luchar todos los días. Y si dejamos de construir las condiciones en las que prospera, la democracia dejará de existir. La privacidad es importante porque empodera a la ciudadanía. Protégela.

Google puede saber qué es lo que te mantiene despierto por la noche, qué es lo que más deseas y qué planeas hacer mañana

REFERENCIAS BIBLIOGRÁFICAS

- Associated Press. "Google Records Your Location Even When You Tell It Not To". *The Guardian*, 13 agosto de 2018.
- Brunton, Finn y Nissenbaum, Helen. *Obfuscation. A User's Guide for Privacy and Protest*. Cambridge: MIT Press, 2015.
- Dreyfus, Hubert y Rabinow, Paul. *Michel Foucault. Beyond Structuralism and Hermeneutics*. University of Chicago Press, 1982.
- Flyvbjerg, Bent. *Rationality and Power. Democracy in Practice*. Chicago University Press, 1998.
- Forst, Rainer. "Noumenal Power." *The Journal of Political Philosophy*, vol. 23, n.º 2, 2015, p. 111-27.
- Lukes, Steven. *Power. A Radical View*. Red Globe Press, 2005.
- Peterson, Andrea. "Snowden Filmmaker Laura Poitras: 'Facebook Is a Gift to Intelligence Agencies'". *The Washington Post*, 23 de octubre de 2014.
- Véliz, Carissa. "Inteligencia Artificial: ¿Progreso O Retroceso?". *El País*, 14 junio de 2019a.
- "Privacy Is a Collective Concern". *New Statesman*, 22 de octubre de 2019b.
- "Privacy Is Power". *Aeon*, septiembre de 2019.
- Weber, M. *Economy and Society*. Berkeley: University of California Press, 1978.
- Zuboff, Shoshana. *The Age of Surveillance Capitalism*. London: Profile Books, 2019.

10. Véase Brunton y Nissenbaum, 2015.

11. Véase Véliz, 2019b.