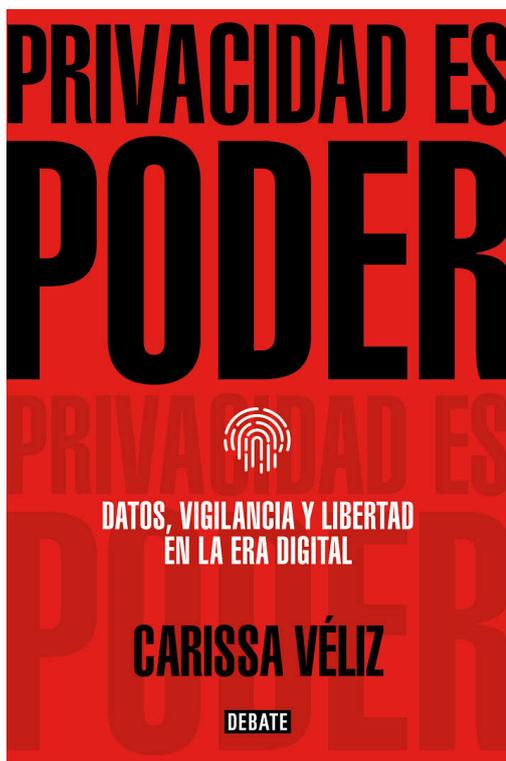


Felipe A. López



Carissa Véliz

Privacidad es Poder. Datos, vigilancia y libertad en la era digital

Editorial Debate, 2021, pp. 299

Con la pandemia del Covid-19, han proliferado las herramientas de seguimiento, trazabilidad y control implementadas por los gobiernos, las que van desde carnet de vacunación, permisos de desplazamientos e incluso aplicaciones instaladas en nuestros móviles, con acceso a más de un dato privado, entre ellos la geolocalización y en las cuales, los datos son almacenados fuera de sus fronteras, levantándose varias banderas de alerta ante esta pérdida de privacidad producto de una “necesidad mayor” aun cuando su utilidad es al menos discutible (Arancibia-Collao & San Martín, 2021).

Así también, permitió visibilizar problemas de seguridad, que afectan nuestra privacidad, entre ellos, el caso de Zoom, quienes aseguraban poseer más seguridad que la realmente implementada. Por otro lado, las universidades han dispuesto aplicaciones, con políticas de privacidad poco claras y dónde no se tiene certeza de que se cumpla un adecuado resguardo a la información que obtienen, e incluso han sido atacadas con discontinuidad de su operación como las Universidades de Castilla-La Mancha y Autónoma de Barcelona.

**INFORMACIÓN:**

<https://doi.org/10.46652/pacha.v3i7.91>  
ISSN 2697-3677  
Vol. 3, No. 7, 2022. e21091  
Quito, Ecuador

Enviado: marzo 03, 2022  
Aceptado: abril 15, 2022  
Publicado: abril 20, 2022  
Sección Reseña | Peer Reviewed  
Publicación continua



**AUTOR:**

Felipe A. López  
Universidad Academia de Humanismo Cristiano - Chile  
felipe.lopez@uacademia.cl

**CONFLICTO DE INTERESES**

El autor declara que no existió conflicto de interés posible.

**FINANCIAMIENTO**

No existió asistencia financiera de partes externas a la presente reseña.

**NOTA**

N/A

ENTIDAD EDITORA

Aun con todos estos casos, sigue pareciéndonos que la privacidad es un tema solo del derecho y la informática, con poca relevancia en otras áreas del conocimiento y aun menos para el ciudadano común. Prueba de esto, es lo señalado por Abou Allaban et al. (2020), quienes indican que los adultos mayores, estarían dispuestos a tolerar menores niveles de privacidad a cambio de lograr una mayor autonomía en el hogar. Lo anterior nos insta, a tomar conciencia de lo qué esto significa y cuáles son las implicancias, a todo nivel de la sociedad y en todas las áreas del conocimiento.

Es ahí donde “Privacidad es Poder. Datos, vigilancia y libertad en la era digital”, escrito por la Dra. Carissa Veliz, investigadora del Instituto de Ética en IA de la Universidad de Oxford, Inglaterra, cobra importancia. El subtítulo de la edición en inglés “Why and How you should take back control of your data” (Por qué y cómo deberías recuperar el control de tus datos), nos llama a recuperar nuestra privacidad, ya que “para que el capitalismo sea habitable -y compatible con la democracia y la justicia- tenemos que marcarles unos límites” (2021, p. 204).

Contextualizar la relevancia de la Privacidad y cómo afecta (y ha afectado) distintas relaciones sociomateriales, en nuestra opinión, es el objetivo del libro, el cual pasa a ser una lectura interesante para comprender la relevancia del tema, no solo por ser atingente en lo personal, sino también, por sus implicancias en las relaciones con los otros, e incluso con lo no-humano. En especial si consideramos cómo la relación con las tecnologías se ha modificado, estas tecnologías hoy toman decisiones en el hogar, monitorean nuestros signos vitales, nos dicen que ver, nos comunican e incluso nos crean nuevas realidades como el metaverso. Los datos personales se han utilizado en dis-

tintos contextos y episodios históricos, por tanto, la discusión del hoy afectará el mañana, pudiendo dar la historia ejemplos de sus (mal) usos y ayudarnos a forjar un mejor futuro.

La privacidad, esa frontera entre mi yo y los otros, debe ser mantenida, protegida y consolidada como un recurso inexpugnable, considerando la privacidad por defecto y desde el diseño, como base para una relación saludable con las tecnologías y con los otros.

El libro se compone de 6 capítulos, en los primeros 4 la autora, en forma clara pero no menos cruda, nos relata, cómo los datos personales han posibilitado masacres y migraciones forzadas, se han utilizado para perseguir activistas, encarcelar inocentes, ganar elecciones, desinformar a la comunidad y un largo etc., mostrándonos la gravedad del problema, ya no solo en términos personales, sino con claras consecuencias en la sociedad, en la seguridad nacional, en la democracia y en las relaciones con los otros, es decir, en la paz social.

La autora ve la privacidad como un bien público y un activo relevante para mantener una adecuada y sana democracia, por tanto, su protección no puede ser solo individual, sino que debe ser una construcción de la sociedad. Vemos de este modo, que se perfila como un objeto sociotécnico, mediando entre distintos componentes de la sociedad, pero también estabilizando ciertas relaciones.

Una de las formas estabilizadas, es el capitalismo de datos, de la cual la autora nos señala, que las empresas tecnológicas escaparon de las autoridades antimonopolio, ya que la forma tradicional de medir es por el precio y su influencia sobre este, ahora bien, al ser gratuitas no extraen el excedente del consumidor, sino que todos sus datos, con un canibalismo de da-

tos. El llamado en este caso, es a comprender estas nuevas organizaciones y su relación con el trabajo, en especial en su forma oculta de explotación -de datos (Valdebenito Allendes, 2018), más allá que en su capacidad de controlar precios.

Esta modificación del capitalismo, en palabras de Mayer-Schönberger & Ramge (2019), implica que en mercados ricos en datos, no se utilizará el precio como información y por tanto el dinero perderá el poder que hoy tiene, afectando todas las relaciones comerciales. Por tanto, se pasará de un capital financiero a un capital cibernético (Sai, 2021).

Estas nuevas formas de comercio, que no necesariamente implica intercambio de dinero, en la cual el trueque de datos pasa a ser una actividad cotidiana entre las empresas, sin considerar a los usuarios, dado la asimétrica relación de poder, el usuario no tiene información de qué datos le extraen, cómo se utilizan y cómo luego lo influncian.

Otro punto relevante, es cómo la pérdida de la privacidad va socavando la democracia, si bien, presenta el caso de Cambridge Analytica no sé queda en este, sino que muestra otras formas, en que, mediante datos de las personas, se persuaden a los votantes e incluso les crean nuevos contextos y realidades, con lo cual los consensos, tan necesarios en democracia, se hacen impracticables. Lo anterior mediante anuncios dirigido en función de gustos y comportamientos en la red.

Esta publicidad oscura o personalizada, no solo afecta la forma en que nos relacionamos, sino también, cómo interactuamos con problemas globales como la pandemia y el cambio climático, por lo que se insta a dejar este tipo de

publicidad y regularla de una forma amplia y creativa (pensando en los futuros), más allá de si la información está anonimizada o no.

Esto último especialmente sensible con los datos de salud y genéticos, usados por ejemplo en la investigación de De Saint Pierre et al. (2020), quienes mediante ADN, realizaron un Análisis histórico genético de la población de la región de Antofagasta, estas investigaciones deben dar garantías que la información será custodiada adecuadamente y borrada cuándo se solicite, en especial utilizando métodos de encriptación o seudomización. Sin embargo, conocemos los métodos de decodificación actuales, pero aún no intuimos los que se generen, por ejemplo, con la computación cuántica.

El quinto capítulo, nos señala modificaciones que en su opinión deberían emprender las sociedades, entre ellas, dejar la publicidad oscura y la vigilancia algorítmica tanto por privados como por gobiernos, nos da señales de la importancia de la ciberseguridad y de la custodia a los datos médicos y genéticos. En este capítulo plantea que “Solo cuando la resistencia se vuelve persistente, se consigue que las grandes tecnológicas den un paso atrás -después de haber dado varios hacia adelante” (Véliz, 2021, p. 153), esta resistencia es tanto individual como colectiva y por tanto, el llamado es a participar, informarme y presionar para mayor privacidad, ciberseguridad y seguridad de nuestros datos.

El capítulo seis y último, es una caja de municiones, parafraseando a Tomas Ibáñez, en el ámbito de la privacidad individual, dando recomendaciones de herramientas como Signal (para sustituir WhatsApp), Brave (en vez de Chrome) o DuckDuckGo (para reemplazar Google, aunque preferimos [www.ecosia.org](http://www.ecosia.org) ya que además permite cuidar el medio ambiente).

Sin bien, el libro se centra en lo individual, el llamado es a sensibilizar respecto a la privacidad como un objeto social, presionando a políticos y empresas para que custodien de mejor manera los datos privados, mostrando como la regulación europea (RDGP), ha mejorado esta asimetría, señalando sus limitaciones e invitando a la ciudadanía a ejercer mayor presión para su solución.

En Latinoamérica aún estamos lejos de tener una estrategia regional respecto a la privacidad, aun cuando hemos vivido los flagelos de su mal utilización, recordemos que Cambridge Analytica actuó al menos en Argentina, Brasil, Colombia y México, que activistas digitales han sido detenidos en Argentina y Colombia y que el lobby ha obstaculizado y malformado regulaciones sobre privacidad en Chile y otros países.

En nuestra opinión, es necesario que desde la academia se levante la discusión de las implicancias de la privacidad en/para la investigación y de cómo esta disminución de la privacidad genera efectos sociales, dando cuenta de los peligros de la vigilancia algorítmica, los sesgos de las tecnologías y cómo las mismas son utilizadas para nuestra vigilancia y control, considerando que los discursos sobre seguridad son los principales argumentos de los grupos totalitarios, seguridad donde la tecnología emerge como “La solución” (cámaras de vigilancia, drones, aplicaciones de seguimiento, etc.), sin embargo, se acompaña de menos privacidad.

Si como señaló Assange (Assange et al., 2016) “internet, nuestra mayor herramienta de emancipación, se ha transformado en la facilitadora más peligros del totalitarismo jamás vista”, debemos ser capaces de entender como la trans-

formación digital del estado, la disminución de la brecha de internet, y un largo etcétera, se convertirán en nuestra contra al no considerar la privacidad por defecto y desde el diseño.

Por la extensión del libro, no se pueden abordar todos los ámbitos de la privacidad, dónde como planteábamos en la introducción, no se ven los efectos con lo no-humano, en especial si consideramos cómo afecta a los animales con los que vemos TV (siguiendo a Deleuze), y donde sus datos impactan en sus humanos, por ejemplo, un rastreador GPS, podría dar las zonas de tránsito, pudiendo ser abordados.

Otro punto poco abordado, es referente a los sesgos algorítmicos, por lo cual recomendamos revisar el libro de Cathy O’Neill (2016), quien muestra diversos casos de sesgos algorítmicos.

Finalmente, un dato poco estudiado y nada considerado en el libro, es el impacto que este canibalismo de datos tiene en el medioambiente, ya que para su uso se requieren miles de kilómetros de cables, baterías de litio, discos y tarjetas con materiales raros, además de energía y agua en bastante cantidad. Por tanto, el impacto de esta pérdida de privacidad, el aumento en el procesamiento de datos y el abuso en la gestión de información, se han desligado de sus responsabilidades con el medio ambiente, no teniendo el usuario conciencia de la huella de carbono que genera al enviar un emoji o al procesar datos, creyendo incluso que internet, es realmente una nube.

## Referencias

- Abou Allaban, A., Wang, M., & Padir, T. (2020). A Systematic Review of Robotics Research in Support of In-Home Care for Older Adults. *Information*, 11(2), 75. <https://doi.org/10.3390/info11020075>
- Arancibia-Collao, F., & San Martín, E. (2021). El valor de la privacidad en el combate al COVID-19 en Chile: análisis de las tecnologías de trazabilidad. *Temas de La Agenda Pública. Centro de Políticas Públicas UC*, 16(143), 1-17. <https://repositorio.uc.cl/xmlui/bitstream/handle/11534/61663/paper143-25junio.pdf>
- Assange, J., Appelbaum, J., Muller-Maguhn, A., & Zimmermann, J. (2016). *Cypherpunks Freedom and the future of the internet*. Or Books.
- de Saint Pierre Barrera, M., Faure Echeverría, M., & Morales, H. (2020). Análisis histórico genético de la población de la región de Antofagasta revela discontinuidad en la costa y valles interiores. *Estudios Atacameños*, (64), 183-198. <https://doi.org/10.22199/issn.0718-1043-2020-0007>
- Mayer-Schönberger, V., & Ramge, T. (2019). *La reinención de la economía: El capitalismo en la era del big data*. Turner.
- O'Neill, C. (2016). *Armas de destrucción matemática. Cómo el Big data aumentar la desigualdad y amenaza la democracia*. Capitan Swing.
- Sai, L. F. (2021). ¿Qué es el capital cibernético? *Nueva Sociedad*, 294. <https://nuso.org/articulo/que-es-el-capital-cibernetico/>
- Valdebenito Allendes, J. (2018). Un fantasma recorre la web. Aproximación crítica al trabajo digital y cibervigilancia. *Revista F@ro*, 1(27), 35-59. <https://www.revistafaro.cl/index.php/Faro/article/view/541/510>
- Véliz, C. (2021). *Privacidad es Poder*. Debate.

---

## AUTOR

**Felipe A. López.** Magister en Ciencia, Tecnología y Sociedad (U. Alberto Hurtado - Chile) y Magister en negocios internacionales (U. de Lleida - España), Ingeniero en información y control de gestión (U. de Chile - Chile). Ha sido profesor en temas de gestión de riesgos, seguridad de la información y ciberseguridad en universidades como Universidad Andrés Bello, Universidad Academia de Humanismo Cristiano y Universidad del Bio-Bio.