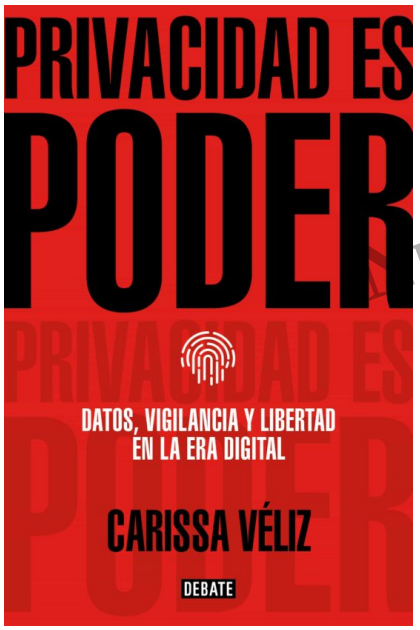
Por qué y cómo se debe recuperar el poder de los datos

Descripción

«Es la hora de recuperar el control. Reclamar la privacidad es la única forma que tenemos de retomar el control de nuestras vidas y nuestras sociedades», subraya **Carissa Véliz** en su nuevo libro, *Privacidad es poder*, editado en español por la editorial Debate.



Privacidad es poder.
Debate. 304 págs. 18,90 € (papel) / 9,49 € (digital).

Para recuperar el derecho a la privacidad que los ciudadanos tenían antes de la llegada de internet, es fundamental, según Véliz, que se regule la actividad de las grandes tecnológicas, como en el pasado se reguló la industria siderúrgica, la automovilística, la farmacéutica o la alimenticia.

> Es fundamental que se regule la actividad de las grandes tecnológicas, como en el pasado se reguló la industria siderúrgica, la automovilística, la farmacéutica o la alimenticia

La filósofa y profesora de la Universidad de Oxford considera que **el actual modelo económico basado en la explotación de los datos personales es tóxico**, no ofrece ventajas para los

ciudadanos, los encierra en guetos informativos, facilita que se les manipule, polariza las visiones del mundo y genera enfrentamientos y dinámicas de desigualdad, pues el acceso a oportunidades o información relevante dependerá del segmento en el que hayan sido catalogados tras el análisis de sus datos.

Por todo ello, el libro *Privacidad es poder* trata de ser una guía para empoderar a los lectores en el camino hacia la recuperación de su privacidad. «La economía de datos y la vigilancia omnipresente de la que se alimenta nos tomó por sorpresa. Las empresas de tecnología no informaron a los usuarios sobre cómo se estaban utilizando nuestros datos, y mucho menos pidieron permiso. **Tampoco preguntaron a nuestros gobiernos.** No había leyes para regular el rastro de datos que dejan los ciudadanos a medida que avanzábamos en un mundo cada vez más digital», reflexiona Véliz en el libro.

«Cuando nos dimos cuenta de qué estaba sucediendo, la arquitectura de la vigilancia ya estaba en su sitio. Gran parte de nuestra privacidad se había ido. A raíz de la pandemia del coronavirus, la privacidad se enfrenta a nuevas amenazas, ya que muchas de las actividades que antes eran *offline* han pasado a ser *online*, y se nos ha pedido que cedamos nuestros datos personales en nombre del bien común. Es tiempo para pensar con cuidado qué tipo de mundo queremos habitar cuando la pandemia sea un recuerdo lejano. Un mundo sin privacidad es peligroso», considera.

La privacidad es necesaria para explorar nuevas ideas en libertad, para tomar nuestras propias decisiones. La privacidad nos protege de presiones indeseadas y de abusos de poder. La necesitamos para ser individuos autónomos, que a su vez son necesarios para que las democracias funcionen bien.

> El libro trata de ser una guía para empoderar a los lectores en el camino hacia la recuperación de su privacidad, que nos ha arrebatado la «economía de datos»

«**Nuestras vidas, traducidas a datos, forman la materia prima de la economía de la vigilancia**. Nuestras esperanzas, nuestros miedos, lo que leemos, lo que escribimos, nuestras relaciones, nuestras enfermedades, nuestros errores, nuestras compras, nuestras debilidades, nuestros rostros, nuestras voces… Todo es usado como forraje por los buitres de datos que lo recopilan todo, lo analizan todo y lo venden al mejor postor», advierte la autora.

Ya es demasiado tarde para prevenir y evitar el desarrollo de la economía de los datos, pero no es demasiado tarde para reclamar nuestra privacidad, según sostiene la autora. A su juicio, de la decisión que tomemos sobre este asunto dependerá el futuro de la humanidad durante las próximas décadas, el modo en el que se desplieguen las campañas políticas, en el que las corporaciones se ganen la vida, el poder que puedan ejercer gobiernos y empresas privadas, el avance de la medicina, la búsqueda de objetivos de salud pública, los riesgos a los que estemos expuestos o la manera de relacionarnos y, no menos importante, de cómo se gestione nuestra privacidad dependerá si se respetan nuestros derechos en el día a día.

En el libro, Véliz analiza el estado actual de la privacidad, cómo creció y llegó a ser lo que es la economía de la vigilancia, los motivos por los que deberíamos acabar con este modelo y cómo hacerlo. Para ello dedica un capítulo a introducir al lector en un día cualquiera en medio del capitalismo de la vigilancia para ilustrarle sobre las dimensiones de la privacidad perdida. En ese viaje, **el lector experimentará cómo se recolectan sus datos cuando paga con tarjeta**

, cuando participa en una videoconferencia, cuando utiliza Facebook u otra red social, cuando compra en la farmacia o va al médico, cuando acude a un organismo que emplea tecnologías de reconocimiento facial, cuando pasa el control para volar en un aeropuerto, atraviesa una frontera o cuando su teléfono móvil tiene activada la geolocalización o es detectado por los repetidores telefónicos más cercanos de la ciudad.

¿CÓMO HEMOS LLEGADO HASTA AQUÍ?

El contraste entre esta situación y la vida que tenían los ciudadanos en los años noventa del pasado siglo es gigantesco. Por eso la autora dedica otro capítulo a responder a la pregunta *How did we get here?* (¿Cómo hemos llegado hasta aquí?). «¿Por qué hemos permitido que la sociedad de la vigilancia eche raíces?», se cuestiona.

La autora considera que el punto de inflexión se produjo cuando grandes tecnológicas como **Google o Facebook** descubrieron que los datos personales resultantes de nuestra vida digital podrían generar muchas ganancias, además de los cambios derivados de los atentados contra las torres gemelas de Nueva York el 11 de septiembre de 2001, y la creencia errónea de que la privacidad es un valor obsoleto.

Carissa Véliz.

> «Cuando nos dimos cuenta de qué estaba sucediendo, gran parte de nuestra privacidad se había ido», asegura Carissa Véliz

Así, según Véliz, el principal protagonista en la historia de la transformación de la huella de nuestros datos en polvo de oro fue Google. La autora recuerda cómo la compañía nació con un algoritmo basado en el sistema de citaciones de las instituciones académicas, gracias a la creatividad y el ingenio de dos estudiantes de Stanford. Los dos jóvenes deseaban al inicio que Google fuerza una herramienta académica. Pero su idea cambió años más tarde. «Desafortunadamente para todos nosotros, el problema fue que Page y Brin (los dos fundadores de Google) quisieron que Google

Search pasara de ser una herramienta asombrosa a una compañía dedicada a hacer dinero», subraya la autora.

A partir de 2001 Page y Brin comenzaron a multiplicar los beneficios de una compañía que hasta entonces no había pasado de ser una *startup* de internet sin beneficio para los inversores. ¿Qué cambió ese año? Los dos jóvenes socios comenzaron a utilizar los datos personales de sus usuarios para vender anuncios publicitarios, inaugurando la era del «**capitalismo de la vigilancia**», como lo ha denominado la psicóloga **Shoshana Zuboff**.

Fue así como nació AdWords, **un sistema para hacer dinero a través de los anuncios publicitarios dirigidos a los usuarios** en función de sus intereses, desvelados a través de sus búsquedas. El sistema pronto cambió el modelo de negocio de Google: los usuarios dejaron de ser los clientes, que a partir de entonces fueron los anunciantes. Los usuarios serían, desde ese momento en adelante, el producto.

«La principal víctima del éxito publicitario de Google fue nuestra privacidad. Nuestros datos, que hasta entonces solo se habían utilizado para mejorar el motor de búsqueda de Google, empezaron a utilizarse para personalizar anuncios. A través de nuestras búsquedas, Google construyó una imagen precisa de nuestras mentes, tanto colectiva como individualmente», señala.

En 2003, el concepto había sido ya suficientemente elaborado, y los ingenieros de Google registraron una patente denominada «Generar información del usuario para su uso en publicidad dirigida». La patente no solo describía cómo usar los datos que el usuario dejaba a través de sus búsquedas para ofrecerle determinada publicidad. También explicaba cómo inferir datos que los usuarios no proporcionaran voluntariamente.

Pronto aparecieron más herramientas, como **Adsense, gracias a la cual el usuario era seguido más allá de sus búsquedas en Google**, colocando anuncios personalizados en webs de todo tipo, no vinculadas en absoluto con el propio Google. «Con Adsense y AdWord, Google había iniciado la economía de la vigilancia», expone la autora. Antes de Google se habían vendido y comprado datos y algunos de ellos se habían usado para la publicidad, pero no a gran escala; no con ese nivel de especificidad y análisis. No con el propósito de personalizar los mensajes. «Google transformó con éxito la huella de datos de los usuarios en polvo de oro e inauguró la economía de la vigilancia como uno de los modelos de negocio más lucrativos de todos los tiempos», concluye Véliz.

> «Con la pandemia, la privacidad se enfrenta a nuevas amenazas, ya que muchas actividades han pasado a ser online, y se nos ha pedido que cedamos nuestros datos personales en nombre del bien común»

Más tarde llegarían otros productos como **Gmail, Chrome, Maps, Pixel, Nest o DoubleClick**, entre muchos otros, que servirían como vías de recolección masiva de datos de los usuarios. Los gobiernos no reaccionaron. Y los usuarios creyeron que les estaban ofreciendo múltiples servicios de manera gratuita y consideraron que aquello era una ganga.

PRIVACIDAD POR SEGURIDAD

Otro suceso determinó la extensión absoluta de la economía de la vigilancia: los atentados contra las

torres gemelas el 11 de septiembre de 2001. Después de aquella masacre que conmocionó al mundo, el foco de la acción del Gobierno de los Estados Unidos pasó a ser la seguridad. Las incipientes regulaciones que se habían promovido años antes en torno al uso de las *cookies* y los datos de los usuarios fueron archivadas.

Pero no se trató únicamente de un tema de prioridades. Las agencias de inteligencia vieron una oportunidad para expandir sus poderes de vigilancia haciéndose con copias de todos los datos personales que las grandes corporaciones estaban obteniendo. Una vez que el Gobierno prestó interés a nuestros datos personales, desaparecieron los incentivos para regular nuestra privacidad, según relata Véliz. Más bien al contrario: a más datos recolectados por las empresas, mayor poder de vigilancia del Gobierno y más ataques terroristas podrían prevenirse.

El Congreso de los Estados Unidos aprobó numerosas iniciativas relacionadas con la vigilancia que permanecieron secretas: leyes, tribunales, políticas. Para un ciudadano corriente, era imposible saber cómo estaba funcionando el sistema de libertades y vigilancia en ese país, hasta que, en 2013, **un empleado de la National Security Agency (NSA) se convirtió en denunciante de todo un entramado de vigilancia** sobre la información de tipo personal de los ciudadanos.

La NSA recolectó datos de Microsoft, Yahoo, Google, Facebook, YouTube, Skype y Apple, entre otras compañías, a través de un programa denominado PRISM. Esto incluyó correos electrónicos, fotos, vídeo y audio chats, historiales de búsqueda y todos los datos almacenados en nuestras nubes. «Por si eso no fuera suficiente, la NSA también recopiló datos en sentido ascendente, es decir, recopiló datos directamente de la infraestructura de internet del sector privado, desde enrutadores hasta cables de fibra óptica», denuncia.

Después de esto, la NSA empleó un sistema llamado XKEYSCORE para organizar todos los datos que había recogido. Dicho sistema era una especie de motor de búsqueda que permitía a los analistas escribir la dirección, el teléfono móvil o la dirección IP de cualquier persona y revisar toda su actividad reciente en línea. También podían ver a las personas en vivo mientras se conectaban y leer lo que tecleaban, letra por letra.

> La agencia de seguridad americana dispone de medios para desplegar una vigilancia aún más intrusiva en el caso de personas a las que se desee hacer especial seguimiento

La agencia de seguridad americana dispone de medios para desplegar una vigilancia aún más intrusiva en el caso de personas a las que se desee hacer especial seguimiento. La NSA puede además compartir los datos recolectados con otras agencias de seguridad internacionales. «A la comunidad de inteligencia le gusta denominar tal invasión de la privacidad “recopilación masiva de datos” para evitar su nombre sencillo: vigilancia masiva», concluye la autora.

VIGILANCIA MASIVA Y TERRORISMO

«Lo más lamentable de nuestra pérdida de privacidad es que no ayudó a prevenir el terrorismo. La idea de que si disponemos de más datos de la gente estaremos preparados para prevenir cosas como el terrorismo es una intuición. El atractivo es comprensible, pero es un error. Cada pieza de evidencia que tenemos sugiere que la vigilancia masiva en los Estados Unidos ha sido absolutamente inútil para prevenir el terrorismo», lamenta. De hecho, Véliz recuerda que el Grupo del Presidente para la

Revisión en Inteligencia y Tecnologías de la Comunicación no pudo encontrar un solo caso en el que las escuchas telefónicas almacenadas hubieran detenido un ataque terrorista. «Recopilando mucha más información irrelevante que relevante, la vigilancia masiva añade más ruido que señales», subraya.

En las dos décadas en las que lleva funcionando este sistema de vigilancia masiva, según la autora, este no ha demostrado que sirva para prevenir el terrorismo, «pero **ha sido muy eficaz para eliminar el derecho a la privacidad de todos los usuarios de internet**».

A juicio de Véliz, pueden extraerse algunas lecciones de este lamentable episodio de la historia reciente. La primera es que la sociedad de la vigilancia nació de la colaboración entre instituciones públicas y privadas. Los gobiernos permitieron que la recolección de datos por parte de las corporaciones prosperase para hacer una copia de los datos.

La economía de los datos fue tolerada porque proporcionó un nuevo recurso para ejercer el poder a los gobiernos. Como contrapartida, las corporaciones asistieron a dichos gobiernos a la hora de desplegar sus sistemas de vigilancia. Así sucedió con **AT&T y la NSA americana, o con Palantir, Amazon y Microsoft** y las herramientas de vigilancia de la administración presidida por Donald Trump. La venta de datos entre gobiernos y corporaciones ha dejado finalmente indefensos a los ciudadanos, que no pueden protegerse a un tiempo de los unos y de los otros.

La segunda gran lección se ha aprendido durante la pandemia sufrida tras la extensión del coronavirus por todo el mundo: **las crisis son peligrosas para las libertades civiles.**

«Durante las crisis, las decisiones son tomadas sin considerar cuidadosamente pros, contras, evidencias y alternativas. Siempre que haya alguna resistencia a adoptar medidas extremas, una llamada a salvar vidas silencia a los disidentes. Nadie quiere interponerse en el camino a la hora de salvar vidas, incluso cuando no hay evidencia de que esas iniciativas vayan a salvar vidas», señala.

> Para enmendar la situación, la autora propone acabar con la publicidad personalizada, que ha hecho posible corromper los procesos electorales, entre otras cuestiones

En ese contexto, según la autora, las libertades civiles son sacrificadas injustificadamente sin ninguna garantía de que volverán después de la crisis. Las medidas extraordinarias adoptadas durante la ola de pánico tienden a permanecer mucho tiempo después de que la emergencia haya finalizado.

«PRIVACY IS POWER»

La privacidad significa el poder de influir sobre las personas. **Podemos creer erróneamente –según la autora– que nuestra privacidad está a salvo porque no somos nadie en especial**, no somos personajes relevantes. Pero siendo quienes somos tenemos el poder de prestar atención, algo por lo que las compañías tecnológicas están luchando, incluso investigando sobre la dopamina que generan nuestros cerebros ante determinadas *apps*, buscando generar adicción. Tenemos dinero, aunque sea poco. Tenemos un cuerpo, una identidad, conexiones con otras personas, y tenemos la posibilidad de votar y decidir sobre los demás. «Como ves, eres una persona muy importante. Eres una fuente de poder», subraya la autora dirigiéndose al lector.

El poder es más valioso que el dinero. Y, según Véliz, es similar a la energía, en el sentido de que puede transformarse una y otra vez, pasando de poder económico a poder político, y de este a la capacidad de ganar dinero de nuevo. La relación entre poder y privacidad en la era digital ha dado lugar a un tipo de dominación que tiene que ver con las relaciones entre poder y conocimiento.

«El poder crea conocimiento y decide qué se considera conocimiento», subraya Véliz en alusión al papel que ha adquirido Google en nuestra sociedad. Además, cuanto más sabe alguien sobre nosotros, más puede anticiparse a cada movimiento, y de esa forma más puede influir sobre nosotros. Cuanto más invisible sea ese poder, más poderoso es.

El poder de anticiparse a los movimientos de las personas y de influir sobre ellas, derivado del acceso a sus datos personales, es la quintaesencia del poder en la era digital. Los gobiernos saben más sobre sus ciudadanos de lo que nunca antes han sabido. Los servicios de inteligencia de la Alemania comunista, por ejemplo, únicamente lograron tener archivos de un tercio de la población de Alemania oriental. Hoy las agencias de inteligencia disponen de mucha más información de toda la población. Mucha de ella procede de las propias redes sociales, y entre otras posibilidades permite a los gobiernos anticiparse a determinadas protestas e incluso arrestar a sus responsables de manera preventiva. Tener el conocimiento de qué planes tiene la resistencia antes de que ocurran y estar preparado para golpearles a tiempo es –según la autora– el sueño de cualquier tirano.

El uso de los datos personales es el amianto del siglo XXI: como sucede con ese material, se consigue y se utiliza fácilmente y puede ser vendido e intercambiado. Y, como sucede con el amianto, también es tóxico. **Son numerosos los ataques de *hackers* que roban datos** y los emplean para cometer extorsiones y diferentes delitos. El acceso a nuestros datos ofrece ventajas a nuestros adversarios y competidores y nos convierte en seres completamente vulnerables.

TIRANDO DEL ENCHUFE

Tras el análisis, Véliz concluye que es preciso poner punto y final a este mercadeo de datos personales. Según la autora, es un objetivo posible, como lo es reducir y eliminar el agujero en la capa de ozono en un determinado período de años gracias al esfuerzo colectivo. Pero para lograrlo, en el caso de los datos personales, es precisa una regulación, y para ello es necesario persuadir a quienes tienen el encargo de legislar, a los constructores de las políticas públicas, a los políticos. Y para llegar a ellos se necesita una opinión pública sensibilizada acerca de la importancia de preservar la privacidad.

Una de las medidas que deben adoptarse para enmendar la situación es, según la autora, acabar con la publicidad personalizada. Ese tipo de publicidad ha hecho posible corromper los procesos electorales, entre otras cuestiones. La publicidad tradicional suponía una inversión cuantiosa sin un conocimiento claro sobre la efectividad de los mensajes. La publicidad enfocada promete eliminar la incertidumbre de los anunciantes mostrando a los consumidores solo aquello que les interesa, y ofreciendo a las empresas la seguridad de que solo pagarán por anuncios que van a incrementar sus ventas. En resumen: una garantía de eficiencia.

Pero, según Véliz, «esa es la teoría: una situación *win-win* (ganar-ganar). Desafortunadamente, la práctica no coincide con la teoría. La práctica ha normalizado la vigilancia. Ha provocado la difusión de noticias falsas y del *clickbait.* Ha fracturado la esfera pública e incluso ha comprometido nuestros

procesos democráticos».

Para revertir la situación también debería detenerse la compraventa de datos personales. **La autora aboga por establecer prohibiciones desde los gobiernos, permitiendo solo el intercambio de datos necesarios**, como los compartidos en el seno del sistema de salud, y de datos no personales, empleados para el desarrollo de políticas adecuadas de colaboración e innovación. «Necesitamos definiciones más precisas de lo que cuenta como datos personales», señala, advirtiendo de que es indispensable delimitar también qué datos deben ser anónimos y cuáles no.

La autora también insta a terminar con la recopilación indiscriminada de datos personales sin el permiso de los usuarios. Esto comenzó porque las grandes tecnológicas adoptaron la filosofía de «moverse rápido», más rápido que los usuarios, a los que hicieron creer que recopilar sus datos era indispensable para el correcto funcionamiento de sus *gadgets* y *apps*. Cuando ya era demasiado tarde, las legislaciones han comenzado a referirse al uso de los datos, pero no a su recopilación. Se permite la recogida con fines legítimos, «¿pero qué son fines legítimos?», se cuestiona Véliz. Además, la configuración por defecto de muchos dispositivos lleva a la recolección indiscriminada de datos, y muchos usuarios jamás modificarán esa configuración por defecto.

> «Se ha normalizado la vigilancia, la difusión de noticias falsas y del clickbait, la fractura de la esfera pública e incluso se han comprometido nuestros procesos democráticos»

Por ese motivo, **Véliz aboga por trabajar en «soluciones creativas»** para la recogida de datos respetando la privacidad, y pone como ejemplo métodos como el de privacidad diferenciada, que utiliza algoritmos matemáticos para extraer datos respetando dicha privacidad.

Igualmente habría que detener las inferencias en torno a nuestro comportamiento que han proliferado entre las empresas e instituciones. **Los *likes* de Facebook, por ejemplo, se utilizan para inferir la orientación sexual, la etnia, la religión y los puntos de vista políticos**, los rasgos de personalidad, la inteligencia, la felicidad, el uso de sustancias adictivas, la edad, el género o la separación de los padres. Los patrones de movimiento ocular pueden usarse para detectar dislexia. Nuestros post en Twitter y nuestras expresiones faciales para descubrir depresiones. Incluso se puede inferir si tenemos problemas de memoria por cómo de rápido tecleamos en los teléfonos móviles, los errores que cometemos o a qué velocidad descendemos en la visualización de nuestra lista de contactos.

«La lista continúa, pero ya tenemos el dibujo: señales externas están siendo sistemáticamente utilizadas por compañías e instituciones para inferir información privada sobre nosotros», denuncia Véliz. No tenemos control sobre estas señales externas, que son recogidas a menudo sin nuestro consentimiento. Un punto crítico en torno a este tipo de inferencias es que pueden estar equivocadas, pero a pesar de ello pueden usarse en contra de nuestros intereses. Las inferencias basadas en algoritmos –recuerda la autora– son probabilísticas. Solo aciertan en algunas ocasiones.

Nuestros datos personales no deberían usarse como un arma en contra de nuestros propios intereses. «Para lograr este objetivo, debemos comprometer a las instituciones que recaban y administran datos personales con deberes fiduciarios», según la autora. Véliz recuerda que muchas profesiones tienen este deber de cuidado respecto a sus clientes, como sucede con la medicina o la abogacía.

INCREMENTAR LA CIBERSEGURIDAD

Los deberes fiduciarios protegen a los clientes que se encuentran en una posición de debilidad respecto a los profesionales que supuestamente deben servirles pero que pueden tener intereses en conflicto. Este tipo de deberes, por tanto, son apropiados cuando se da una relación económica en la que hay una asimetría de poder y conocimiento, y en la que un profesional o una compañía pueden tener intereses que vayan en contra de los intereses de sus clientes.

Otra medida que Véliz propone en el libro es incrementar los estándares de ciberseguridad, algo que exige mayores esfuerzos por parte de los gobiernos, y que de no hacerse pone en riesgo la seguridad de ciudadanos, empresas e instituciones.

Junto con todo lo anterior, **la autora aboga por eliminar todos los datos personales recopilados de manera subrepticia e ilegítima**. «Incluso en el caso de datos personales recopilados con fines legítimos, debería existir siempre un plan para su destrucción», subraya.

Además, sería preciso capacitar a los ciudadanos para que puedan hacer un seguimiento de quiénes y por qué tienen sus datos personales. Para ello es necesario abordar algunos desafíos técnicos para garantizar que siempre se solicite el consentimiento de la persona sobre la que versan los datos, y que podamos estar completamente informados acerca de cómo estos datos se están utilizando sin poner en peligro nuestra privacidad. De igual modo, la vigilancia por parte de los gobiernos no debería producirse sin las necesarias garantías, y solo cuando sea absolutamente necesario. La autora aboga además por prohibir determinados equipamientos, financiar las políticas de protección de la privacidad, actualizar las leyes antimonopolio y establecer unas especiales protecciones sobre la infancia.

Todos podemos hacer algo para recuperar nuestra privacidad, según la autora, y de ello dependen nuestras vidas, nuestras libertades y nuestras sociedades democráticas. **«¿En qué tipo de sociedad te gustaría vivir?», interroga la autora al lector.** La respuesta es la elección entre una versión extrema de la sociedad de la vigilancia en la que vivimos ahora, o un mundo en el que la privacidad se respete y eso nos permita ser libres y vivir sin miedo,

Fecha de creación
22/12/2021
Autor
Marta Sánchez Esparza