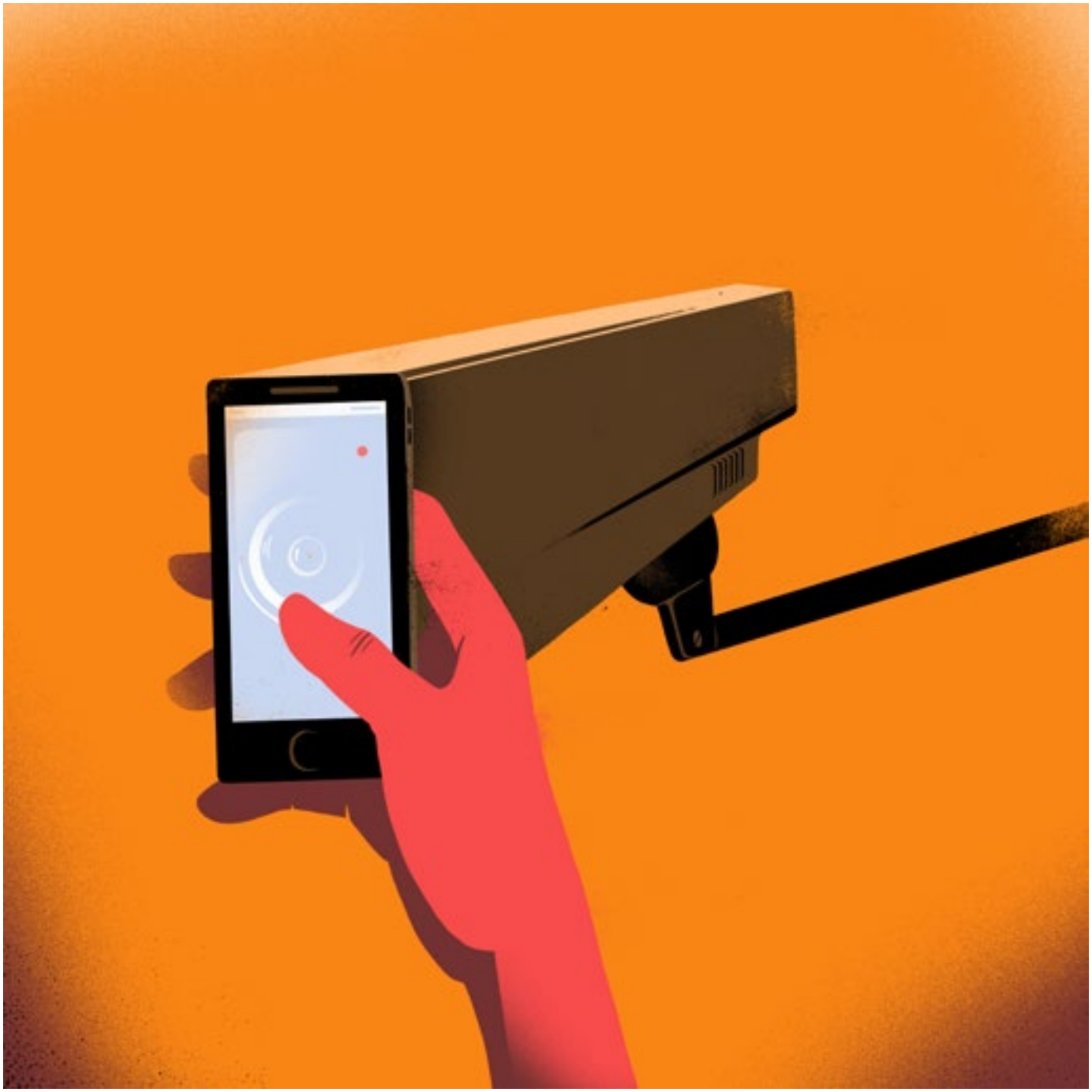


GIGANTES DE LA VIGILANCIA:

LA AMENAZA QUE EL MODELO DE NEGOCIOS DE GOOGLE Y FACEBOOK REPRESENTA PARA LOS DERECHOS HUMANOS

AMNISTÍA INTERNACIONAL

Amnistía Internacional es un movimiento global que cuenta con más de 7 millones de personas que luchan por un mundo donde los derechos humanos estén garantizados para todos.

Nuestra visión es que todos podamos gozar de los derechos humanos establecidos en la Declaración Universal de los Derechos Humanos y en otras normas internacionales de derechos humanos.

Somos una organización independiente de todo gobierno, ideología política, interés económico o religión, y toda financiación proviene de nuestro programa de membresías y de donaciones públicas.

Primera publicación en 2019 por Amnesty International Ltd Peter Benenson House, 1 Easton Street, Londres WC1X 0DW, RU

Todas las imágenes: © Sebastien Thibault/agoodson.com

Índice: POL 30/1404/2019
Idioma original: Inglés
amnesty.org

AMNISTÍA INTERNACIONAL

GIGANTES DE LA VIGILANCIA:

LA AMENAZA QUE EL MODELO DE NEGOCIOS DE GOOGLE Y FACEBOOK REPRESENTA PARA LOS DERECHOS HUMANOS

ÍNDICE

1. RESUMEN EJECUTIVO

La Internet ha revolucionado nuestro mundo a un nivel que no se ha visto desde la invención de la electricidad. Más de la mitad de la población mundial hoy depende de Internet para leer las noticias, comunicarse con sus seres queridos, encontrar un trabajo o resolver consultas urgentes. Asimismo, la Internet ha abierto la puerta a nuevas oportunidades sociales y económicas a una escala y una velocidad casi impensadas hace cincuenta años.

Como reflejo de este cambio, en general, hoy se reconoce que tener acceso a Internet es vital para el pleno ejercicio de los derechos humanos. Para más de 4000 millones de personas, Internet se ha vuelto un elemento central en su forma de comunicarse, aprender, integrarse a la economía y organizarse social y políticamente.

Sin embargo, la participación de estos miles de millones de personas en línea depende fuertemente de los servicios de solo dos corporaciones: dos compañías controlan los principales canales que utilizan las personas en Internet. Además, estas dos compañías ofrecen servicios tan esenciales que es difícil imaginar hoy el mundo cibernético sin ellas.

Por un lado, Facebook es la principal empresa de redes sociales en el mundo. Al combinar los usuarios de su plataforma de redes sociales, sus servicios de mensajería (WhatsApp y Messenger) y aplicaciones como Instagram, un tercio de la humanidad usa a diario un servicio que pertenece a Facebook. De esta manera, Facebook determina buena parte de las conexiones humanas durante esta era digital.

Por otro lado, Google domina una porción incluso mayor del mundo digital. Los motores de búsqueda son una fuente vital de información, y Google acapara casi un 90 % del uso de motores de búsqueda a nivel global. Su navegador, Chrome, domina el campo de navegadores web en todo el mundo. Su plataforma de videos, YouTube, es el segundo motor de búsqueda más grande del mundo, así como la principal plataforma de videos a nivel global. Su sistema operativo para dispositivos móviles, Android, se encuentra en la vasta mayoría de los *smartphones* del mundo.

La hegemonía de Android es particularmente importante, visto que los *smartphones* han reemplazado a las computadoras y hoy son la principal fuente de acceso a Internet. Los *smartphones* revelan información sobre nosotros que va más allá de nuestros hábitos de navegación: por ejemplo, muestran nuestros patrones de desplazamiento físico y nuestra ubicación. También suelen contener miles de mensajes de texto y correos privados, fotografías, contactos y entradas de calendario.

Google y Facebook han ayudado a conectar el mundo y han brindado servicios cruciales a miles de millones de personas. Para tener una participación significativa en la sociedad y la economía actual, las personas dependen de su acceso a Internet y de las herramientas que Google y Facebook ofrecen.

Pero, más allá del valor real de sus servicios, las plataformas de Google y Facebook implican un costo sistémico. Su modelo de negocios basado en la vigilancia acorrala a las personas en un pacto faustiano, por el cual solo pueden disfrutar del pleno ejercicio de sus derechos humanos en línea sometiéndose a un sistema fundado sobre la base del abuso de los derechos humanos. En principio, esto se manifiesta en un ataque de una escala sin precedentes al derecho a la privacidad, seguido de un efecto en cadena que plantea un grave riesgo para otros derechos diversos, desde la libertad de expresión y opinión hasta la libertad de pensamiento y el derecho a la no discriminación.

Esta no es la Internet a la que nos sumamos en un principio. Cuando Google y Facebook recién estaban

empezando, hace casi veinte años, ambas empresas tenían modelos de negocios radicalmente diferentes que no dependían de la vigilancia constante. La erosión gradual de la privacidad en manos de estas empresas es el resultado directo del dominio hegemónico del mercado y del control sobre la versión moderna y global de la "plaza pública" que han sabido establecer.

En el Capítulo 1 de este informe, "El negocio de la vigilancia", se analiza cómo funciona el modelo de negocios basado en la vigilancia: Google y Facebook ofrecen servicios a miles de millones de personas sin pedirles que paguen un precio en dinero por ello. En cambio, los ciudadanos pagan el costo de estos servicios con sus datos personales íntimos. Luego de recopilar estos datos, Google y Facebook los utilizan para analizar a las personas, segmentarlas por grupos y hacer predicciones sobre sus intereses, sus características y, en última instancia, su comportamiento; el principal objetivo es poder usar esta información valiosa para generar ingresos por publicidad.

El aparato de vigilancia va mucho más allá de la barra de búsqueda de Google o de la plataforma misma de Facebook. Los usuarios están bajo el rastro de estas empresas, tanto en las aplicaciones en sus teléfonos como en el mundo físico, seguidos paso a paso a medida que realizan sus tareas día a día.

Estas dos empresas recopilan una gran cantidad de datos relacionados con qué buscamos en Internet, adónde vamos, con quiénes hablamos, qué leemos y, mediante los análisis que hoy son posibles por los avances tecnológicos, tienen el poder de inferir cuál puede ser nuestro estado de ánimo, nuestra etnia, nuestra orientación sexual, nuestra opinión política y nuestra mayor vulnerabilidad. Algunas de estas categorías, incluidas características protegidas por los derechos humanos, se ponen a disposición de terceros con el propósito de segmentar a los usuarios de Internet para brindarles anuncios e información de forma dirigida.

En el Capítulo 2, "Ataque a la privacidad", veremos cómo esta actividad de vigilancia constante y omnipresente ha socavado la mismísima esencia del derecho a la privacidad. No solo representa una intrusión en la vida privada de miles de millones de personas a una escala que bajo ningún punto de vista es necesaria ni proporcionada, sino que además las empresas han condicionado el acceso a sus servicios mediante la imposición de que los usuarios den su "consentimiento" para que se procesen y compartan sus datos personales con fines de marketing y publicidad, en directa violación al derecho a decidir cómo y cuándo se pueden compartir nuestros datos personales con terceros. Por último, las empresas utilizan sistemas algorítmicos para crear e inferir perfiles detallados de las personas, y esto interfiere con nuestra capacidad de construir nuestra propia identidad dentro de un círculo privado.

Inicialmente, los beneficiarios de esta información eran los anunciantes, pero, una vez creadas, estas bóvedas de datos también resultaron una tentación irresistible para los gobiernos. La razón salta a la vista: Google y Facebook alcanzaron un nivel de extracción de datos de sus miles de millones de usuarios que habría sido intolerable si hubiese provenido directamente de los gobiernos. Ambas empresas se han enfrentado a los esfuerzos gubernamentales de obtener información sobre sus usuarios; sin embargo, la oportunidad de acceder a esos datos ha generado una gran falta de incentivo entre los gobiernos para regular la vigilancia corporativa.

El abuso a la privacidad que cimienta el modelo de negocios basado en la vigilancia sobre el cual se erigen Facebook y Google queda de manifiesto al ver la larga trayectoria de estas empresas con los escándalos de privacidad. A pesar de que las empresas aseguran que tienen un fuerte compromiso con la privacidad, es difícil hacer la vista gorda frente a estas numerosas violaciones a la privacidad que son parte del funcionamiento estándar del negocio, no aberraciones esporádicas.

En el Capítulo 3, "Analítica de datos a gran escala: riesgos para los derechos humanos más allá de la privacidad", exploraremos cómo las plataformas de Google y Facebook no solo dependen de la recopilación de enormes cantidades de datos de los usuarios, sino que se basan en extraer más información valiosa y detallada de esos datos utilizando sistemas algorítmicos sofisticados. Estos sistemas están diseñados para encontrar la mejor forma de obtener resultados en beneficio de los intereses de las empresas, que incluyen la segmentación de audiencias y la entrega de publicidad acorde, así como pequeños estímulos conductuales para mantener a las personas interesadas en las plataformas. Como resultado, los datos de las personas, una vez agrupados, se convierten en un instrumento en su contra que se manifiesta de maneras muy diversas e inesperadas.

Se ha visto que estos sistemas algorítmicos generan efectos en cadena que plantean graves amenazas para los derechos de las personas, entre ellos, la libertad de expresión y de opinión, la libertad de pensamiento,

y el derecho a la igualdad y a la no discriminación. Estos riesgos se ven exacerbados por el tamaño y el alcance de las plataformas de Google y Facebook, que pueden socavar los derechos humanos a escala masiva. Además, los sistemas que dependen de analíticas de datos complejas pueden ser difíciles de entender incluso para los expertos en ciencias de la computación, ni mencionar para los miles de millones de personas a quienes pertenecen los datos que se están procesando.

El escándalo de Cambridge Analytica, donde se minaron los perfiles de Facebook de 87 millones de personas para microsegmentar y manipular a los usuarios durante una campaña política, abrió la puerta para que todo el mundo fuera testigo de las capacidades de estas plataformas para influir en la población a gran escala, así como de los riesgos de abuso por parte de otros actores. Y si bien sembró la controversia, este incidente era solo la punta del iceberg, que surge del mismísimo modelo de extracción y análisis de datos inherente a los negocios de Facebook y Google.

Por último, en el capítulo 4, "La concentración de poder, una barrera contra la responsabilización", veremos cómo las vastas reservas de datos y las potentes capacidades de procesamiento han convertido a Google y a Facebook en dos de las empresas más valiosas y poderosas de nuestros tiempos. En contexto, la capitalización de mercado de Google representa más del doble del PBI de Irlanda (donde se encuentran las casas matrices de ambas empresas en Europa), mientras que la de Facebook es un tercio más grande. Su modelo de negocios ha ayudado a concentrar su poder —que incluye el aspecto financiero, su influencia política y la capacidad de moldear la experiencia digital de miles de millones de personas—, y esto ha llevado a una asimetría de conocimientos sin precedentes entre las empresas y los usuarios de Internet: en las palabras de la académica Shoshana Zuboff, "ellos saben todo sobre nosotros; nosotros no sabemos casi nada de ellos".

Esta concentración de poder va de la mano con el impacto que tiene el modelo de negocios sobre los derechos humanos y ha creado un vacío de responsabilización, donde a los gobiernos les resulta difícil imputar las responsabilidades a las compañías, y las personas afectadas encuentran barreras para acceder a la justicia.

Los gobiernos tienen la obligación de proteger a la población de los abusos de derechos humanos perpetrados por las corporaciones. Sin embargo, durante las dos últimas décadas, se ha dejado que las empresas de tecnología prácticamente se autorregulen; en 2013, el ex CEO de Google Eric Schmidt describió al universo cibernético como "el espacio desregulado más grande del mundo". Actualmente, las autoridades nacionales y los entes regulatorios de diversas jurisdicciones han comenzado a adoptar un enfoque más combativo frente al poder concentrado de Google y Facebook, por ejemplo, al investigar a las empresas por presuntas violaciones a las normas de competencia, imponer sanciones por las violaciones al Reglamento General de Protección de Datos (RGPD) de Europa, o implementar nuevos regímenes impositivos para las grandes empresas de tecnología.

Las empresas tienen la responsabilidad de respetar los derechos humanos en el contexto de sus operaciones de negocios, lo que las obliga a implementar procesos de "diligencia debida en materia de derechos humanos" para identificar y mitigar su impacto en ese campo. Google y Facebook han implementado políticas y procesos para mitigar su impacto sobre la privacidad y la libertad de expresión, pero, visto que su modelo de negocios basado en la vigilancia socava la mismísima esencia del derecho a la privacidad y plantea un grave riesgo para otros muchos derechos, evidentemente no han adoptado un enfoque integral y no se han cuestionado si acaso el modelo en sí permite el cumplimiento de sus responsabilidades en torno al respeto por los derechos humanos.

Amnistía Internacional ha dado a Google y Facebook la oportunidad de responder a los hallazgos de este informe previo a su publicación. La respuesta de Facebook está incluida en un anexo al final. Amnistía Internacional conversó con representantes de alto rango de Google, que proporcionaron información respecto de sus políticas y prácticas relevantes. Ambas respuestas han sido integradas a lo largo del informe.

Hoy, es evidente que la era de la autorregulación en el sector de la tecnología está llegando a su fin: se necesitará implementar más regulaciones estatales, pero es vital que, más allá de cómo se presente esta regulación futura del sector, los gobiernos adopten un enfoque basado en los derechos humanos. En el corto plazo, es necesario y sumamente urgente garantizar el cumplimiento de las regulaciones existentes. Los gobiernos deben tomar medidas positivas para reducir los daños que genera el modelo de negocios basado en la vigilancia, como adoptar políticas públicas que tengan como objetivo garantizar el acceso universal y el pleno ejercicio de los derechos humanos; reducir o eliminar la continua vigilancia de entidades privadas; e implementar reformas, incluidas reformas estructurales, que resulten suficientes para reinstaurar la confianza en la Internet.

1. EL NEGOCIO DE LA VIGILANCIA

"No monetizamos lo que creamos... monetizamos a los usuarios".

Andy Rubin, cofundador de Android, 2013[1]

Cada vez que interactuamos en el mundo cibernético, dejamos una huella de información que constituye un registro digital de nuestra actividad. Cuando enviamos un correo electrónico, diversos servidores y centros de datos registran y almacenan cada uno de los datos asociados: el contenido del mensaje, la hora de envío, el destinatario, nuestra ubicación y cientos de datos más. Algo parecido ocurre cuando navegamos por Internet, usamos una aplicación o hacemos una compra con tarjeta de crédito. A medida que realizamos más y más acciones en línea y que se suman más y más dispositivos, servicios e infraestructura conectados a Internet (desde un automóvil hasta una tostadora e incluso una fábrica), la cantidad de datos registrados aumenta de manera constante y exponencial.

1. Steven Levy, Wired, *The Inside Story of the Moto X: The Reason Google Bought Motorola*, 8 de enero de 2013

En parte, la creación de estas huellas de datos es una mera consecuencia del funcionamiento de la tecnología informática, que depende de procesar información digital. Sin embargo, hace tiempo que las empresas de tecnología saben de la importancia que tienen los datos, y de hecho entienden que este "escape de datos" es un recurso de información sumamente valioso. A menudo, se hace referencia a los datos como el "nuevo petróleo". Y si bien la analogía no es tan acertada,[2] sí es cierto que los gigantes de la tecnología han desplazado a las grandes empresas de petróleo en la categoría de las compañías más valiosas del mundo.[3] La recolección y monetización masivas de datos, principalmente con fines publicitarios, ha hecho de la vigilancia el "modelo de negocios de Internet".[4]

El término "datos" puede sonar como un concepto abstracto e intangible. Sin embargo, en pocas palabras, los datos incluyen hechos sobre nuestra vida y nuestro comportamiento y, cuando se procesan y organizan progresivamente, revelan gran cantidad de información sobre nuestros pensamientos más profundos, nuestra conducta y nuestra identidad. Hace tiempo que se reconoce que proteger los datos personales es un paso imprescindible para que podamos ejercer nuestro derecho a la privacidad,[5] un derecho que, a su vez, protege un espacio en el que expresamos nuestra identidad libremente.[6] La intrusión injustificada e indebida en nuestros datos personales constituye una intromisión en nuestra vida privada. Asimismo, atenta contra nuestra capacidad para desarrollar y expresar nuestros pensamientos e ideas de manera independiente, y nos vuelve vulnerables ante la influencia y el control externos.

El presente informe enumera las implicancias para los derechos humanos como consecuencia del modelo de negocios basado en la vigilancia que sustenta a Internet, con especial hincapié en dos empresas: Google y Facebook. En este capítulo se describe cómo estas dos empresas han impulsado un modelo de negocios que consiste en recolectar, analizar y sacar provecho de los datos de las personas, lo que a menudo se conoce como el "capitalismo de la vigilancia".[7] Como resultado, estos gigantes tecnológicos se han repartido el dominio casi total de los principales canales que utilizan las personas para conectarse e interactuar en el mundo digital, y para acceder a la información y compartirla en línea. Así es como dichas empresas se han convertido en los guardianes de la "plaza pública" para gran parte de la humanidad, y semejante posición les concede un poder corporativo inigualable para influir en el ejercicio de los derechos humanos.

EL MODELO DE NEGOCIOS DE GOOGLE Y FACEBOOK

Google y Facebook proveen servicios que generan ingresos a partir de la acumulación y el análisis de datos sobre las personas.[8] En lugar de cobrar una tarifa por sus productos o servicios, estas empresas le exigen a cualquiera que desee utilizarlos que entregue sus datos personales.

Facebook y Google (una subsidiaria del grupo Alphabet Inc) son conglomerados de empresas multinacionales y, como tales, sus operaciones varían considerablemente según cada subsidiaria, producto y servicio. Aun así, ambas empresas comparten el mismo modelo básico de negocios, que consiste en lo siguiente:

a. desarrollar productos y servicios digitales que sean útiles para las personas y recopilar datos exhaustivos acerca de quienes usan estas plataformas o interactúan con ellas. No obstante, tal como se describe en el capítulo 2 más adelante, esto incluye a las personas que se registran en sus plataformas y también a cualquiera que se topa con el invasivo rastreo de datos de dichas empresas en Internet.

---

2. Ver, por ejemplo, Bernard Marr, *Here's Why Data Is Not The New Oil,* Forbes, 5 de marzo de 2018; Jocelyn Goldfein, Ivy Nguyen, *Data is Not the New Oil*, Tech Crunch, 27 de marzo de 2018

3. Statista, *The 100 largest companies in the world by market value in 2019*, agosto de 2019 https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/

4. Bruce Schneier, *Surveillance is the Business Model of the Internet,* abril de 2014, https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html

5. *S y Marper c. el Reino Unido, 30562/04 y 30566/04,* Tribunal Europeo de Derechos Humanos, 4 de diciembre de 2008, y en 1988, en el comentario general 16 sobre el derecho a la privacidad (HRI/GEN/1/Rev. 9 (Vol. I), el Comité de Derechos Humanos (Comité de DD. HH.) afirma que "La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, procesarla y usarla y por que nunca se la utilice para fines incompatibles con el Pacto." (párrafo 10).

6. Comité de DD. HH., *Coeriel y Aurik c. los Países Bajos* (1994), comunicación n.º 453/1991, párrafo 10.2

7. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* 2018 (Zuboff, 2018)

8. Facebook sostiene que sus actividades no están centradas en la recolección de datos sobre las personas y que la recolección de datos no es un objetivo en sí de la empresa, sino que Facebook se mantiene a través de la venta de publicidad. Ver el anexo que se incluye.

b. usar sistemas de algoritmos para analizar la gran cantidad de datos acumulados, asignarles un perfil detallado a las personas y los grupos, y predecir los intereses y comportamientos de los usuarios.

c. vender el acceso a la información a cualquiera que desee dirigirse a un grupo específico de personas. El principal objetivo comercial de estas empresas es vender anuncios para que los mensajes creados por los especialistas en marketing y publicidad lleguen a públicos específicos en Internet.[9] Cabe destacar que estas empresas no venden los datos personales en sí.

Los ingresos totales de Google y Facebook provienen casi en su totalidad de los anuncios, en un 84 % y un 98 % respectivamente.[10] La información que tienen es tan atractiva a los ojos de los anunciantes que a menudo se dice que ambas empresas tienen un "duopolio" en el mercado de la publicidad en línea.[11] Pero no se trata de "anuncios nada más": la información en sus bóvedas de datos, al igual que los conocimientos informáticos que Google y Facebook obtienen de esos datos, es de particular interés para gran cantidad de actores, desde las empresas que establecen tasas de seguro hasta las autoridades de aplicación de las leyes.

El auge del "big data" y el constante seguimiento de la vida de los usuarios en Internet ha dado origen a la "edad de oro de la vigilancia" para los Estados: las autoridades tienen acceso a información detallada sobre la actividad de las personas, algo que era inconcebible antes de la revolución digital.[12] Asimismo, el modelo de negocios basado en la vigilancia que sostiene a Google y Facebook ha prosperado debido a un abordaje bastante laxo de la regulación de la industria tecnológica en países como los Estados Unidos de América, el lugar de origen de ambas empresas (ver capítulo 4).[13] Como consecuencia, desde el año 2001 por lo menos, la vigilancia pública y la privada se han extendido muy rápido y en paralelo.[14]

EL PODER HEGEMÓNICO DE GOOGLE Y FACEBOOK

Los datos conforman un vasto y complejo ecosistema compuesto por una red interconectada de muchos actores diferentes que provienen de una variedad de sectores. De los cinco gigantes de la tecnología (Facebook, Amazon, Apple, Microsoft y Google de Alphabet), Amazon y Microsoft también han adoptado, hasta cierto punto, el modelo de negocios al que se hizo referencia anteriormente.[15] Además, Amazon domina la esfera del comercio electrónico, y tanto este gigante como Microsoft son los principales proveedores de infraestructura de nube del mundo, al punto que alojan gran parte de los datos de la humanidad en sus servidores.[16] Aparte de las marcas más conocidas, existe una gran red de empresas que generan ingresos mediante la explotación de datos: por ejemplo, los "agentes de datos", que acumulan y comercian datos provenientes de una variedad de fuentes, y la industria de la "tecnología publicitaria", que facilita la analítica y las herramientas necesarias para hacer publicidad digital.[17] Por su parte, las empresas de telecomunicaciones también han optado por incorporar tecnología de publicidad dirigida. De hecho, cada vez son más las empresas de diversos sectores que adoptan modelos de negocios basados en datos, similares a los descritos anteriormente.

Sin embargo, Google y Facebook tienen un poder incomparable sobre la vida de las personas en línea, ya que controlan los principales canales que utiliza el mundo entero a la hora de navegar por Internet. Google y

9. Alphabet, *Annual Report on Form 10-K*, 2018, parte 1, ítem 1 disponible en https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm ; Facebook, *Annual Report on Form 10-K*, 2018, parte 1, ítem 1 disponible en https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm

10. Reuters, *Google parent Alphabet's revenue misses estimates, rises at slowest pace in 3 years*, 29 de abril de 2019; Facebook, *Second Quarter 2019 Results*, 24 de julio de 2019

11. Shoshana Wodinsky, *The Digital Duopoly Still Reigns the Ad World*, 22 de marzo de 2019

12. Ambas empresas hicieron referencia a sus políticas y sus informes de transparencia en relación con su respuesta ante algunos pedidos de datos por parte del Estado de acuerdo con estándares de Derechos Humanos. Google, *Legal process for user data requests FAQs*, https://support.google.com/transparencyreport/answer/7381738; Facebook, *Government Requests for User Data,* https://transparency.facebook.com/government-data-requests

13. El experto en ciberseguridad Bruce Schneier dice que "los gobiernos, en realidad, no quieren limitar su propio acceso a los datos haciendo algo en contra de las corporaciones que proveen esos datos". Bruce Schneier, *Data And Goliath*, 2015 (Schneier 2015)

14. Zuboff, 2018, p. 115

15. Los ingresos de Apple provienen en gran medida de la venta de *hardware* y servicios al consumidor.

16. ZDNet, *Top cloud providers 2019*, agosto de 2019 https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/

17. Privacy International, *How do data companies get our data?* 25 de mayo de 2018 https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

Facebook, junto con las distintas empresas de su propiedad, como YouTube y WhatsApp, influyen en las formas en que las personas buscan y comparten información, debaten y participan en sociedad. Sus plataformas se han vuelto fundamentales para la vida moderna y el modo en que las personas interactúan entre sí.

No obstante, hay algunos países que son la excepción, como China. El gobierno chino aplica un "*firewall*" a Internet, un conjunto de controles técnicos que determinan a qué aplicaciones pueden acceder los usuarios y qué sitios web pueden ver. Tales disposiciones hacen de China un caso aparte en la economía de Internet y le permiten al gobierno de este país mantener un régimen represivo de censura y vigilancia en Internet.[18] Como consecuencia, China cuenta con un entorno de servicios de Internet propios, en el que WeChat y Weibo cumplen la mayoría de las funciones que ofrece Facebook, y Baidu aparece como el motor de búsqueda principal en lugar de Google.

Fuera de China, el poder hegemónico de Google y Facebook es claramente evidente en cada una de las siguientes áreas:

- **Redes sociales:** Facebook domina las redes sociales con 2,45 mil millones de usuarios activos en su plataforma principal todos los meses. Esta cifra equivale a casi el 70 % de los usuarios de redes sociales, lo que reduce en gran medida la participación de las empresas rivales.[19]
- **Mensajería:** Junto con Facebook Messenger, WhatsApp, la aplicación de mensajería de propiedad de Facebook, representa el 75 % de la participación de mercado en mensajería para dispositivos móviles fuera de China.[20]
- **Motores de búsqueda:** Google es, por mucho, el motor de búsqueda predominante, ya que más del 90 % de todas las búsquedas en Internet se realizan mediante plataformas de Google.[21] A tal punto es así que el nombre corporativo de la marca es un sinónimo del término "buscar".
- **Video:** YouTube, que pertenece a Google, es el segundo motor de búsqueda más grande del mundo *y* también la plataforma de video más importante.[22]
- **Navegación en Internet:** Google Chrome es el principal navegador en todo el mundo, lo que hace de Google la puerta de entrada a toda la web.[23]
- **Plataformas móviles:** Desarrollado por Google, Android es el principal sistema operativo para móviles en el mundo.[24] Los usuarios de dispositivos con Android suman más de 2500 millones cada mes.[25] Por lo tanto, Google mantiene una presencia constante en el objeto que más nos puede decir sobre la vida de una persona: el *smartphone*.
- **Publicidad:** Juntos, Google y Facebook generan el 60 % de los ingresos de publicidad en línea en todo el mundo,[26] y a ellos corresponde también el 26 % del crecimiento del mercado de la publicidad digital.[27]

---

18. Ver, por ejemplo, Amnistía Internacional, *Annual Report: China Country Profile*, 2017/2018 https://www.amnesty.org/en/countries/asia-and-the-pacific/china/report-china/

19. Facebook, *Información de la empresa,* citando estadísticas de los usuarios del 30 de septiembre de 2019; StatCounter, *Social Media Stats Worldwide*, octubre de 2018 - octubre de 2019 https://gs.statcounter.com/social-media-stats

20. Statista, *Most popular global mobile messenger apps 2019,* julio de 2019 https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

21. Visual Capitalist, *This Chart Reveals Google's True Dominance Over the Web*, abril de 2018 https://www.visualcapitalist.com/this-chart-reveals-googles-true-dominance-over-the-web/

22. Mushroom Networks, *YouTube: The 2nd Largest Search Engine*, 2018 https://www.mushroomnetworks.com/infographics/youtube---the-2nd-largest-search-engine-infographic/.

23. Statista, *Global market share held by internet browsers 2012-2019*, a septiembre de 2019, https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/ .

24. StatCounter, *Mobile Operating System Market Share Worldwide,* octubre de 2018- octubre de 2019 https://gs.statcounter.com/os-market-share/mobile/worldwide

25. VentureBeat, *Android passes 2.5 billion monthly active devices*, mayo de 2019 https://venturebeat.com/2019/05/07/android-passes-2-5-billion-monthly-active-devices/

26. eMarketer, *Digital Ad Spending 2019, marzo de 2019* https://www.emarketer.com/content/global-digital-ad-spending-2019

27. AdExchanger, *Digital Ad Market Soars To $88 Billion, Facebook And Google Contribute 90% Of Growth*, mayo de 2018 https://adexchanger.com/online-advertising/digital-ad-market-soars-to-88-billion-facebook-and-google-contribute-90-of-growth/.

El poder de Google y Facebook sobre las principales plataformas de Internet conlleva riesgos particulares respecto del ejercicio de los derechos humanos, tal como se explica en los siguientes capítulos. Según lo demuestran las estadísticas citadas, a muchas personas les resulta imposible utilizar Internet sin recurrir a los servicios de Google y Facebook.[28] En muchas sociedades, las plataformas de Internet predominantes ya no son "opcionales" y utilizarlas se ha vuelto una parte necesaria de la participación en la vida moderna.

EXTRACCIÓN Y ACUMULACIÓN DE DATOS

Como se ha visto, el modelo de negocios de Google y Facebook se basa, principalmente, en la extracción y acumulación de grandes cantidades de datos de las personas. Estas empresas no se dedican a recopilar nuestros datos solamente; también los utilizan para inferir y crear nueva información sobre nosotros. Las plataformas están basadas en las más recientes herramientas de inteligencia artificial (IA) y aprendizaje automático, las cuales pueden deducir características increíblemente detalladas de las personas y combinarlas en grupos muy específicos.

A fin de aumentar los ingresos generados por los anunciantes, Google y Facebook compiten por ver cuál de las dos marcas ofrece las mejores predicciones acerca de las personas. Para lograr su objetivo, necesitan extender sus bóvedas de datos y perfeccionar sus algoritmos predictivos. Esto incentiva a las empresas a buscar más datos de más personas para así extender sus operaciones en Internet, en el espacio físico y, en definitiva, en el mundo entero.

El enfoque expansionista aplicado a la extracción de datos adopta varias formas diferentes. Primero, las empresas recopilan y almacenan datos sobre las personas de forma exhaustiva.[29] Por ejemplo, de manera predeterminada, Google almacena el historial de búsqueda en todos los dispositivos de un mismo usuario. También guarda información sobre cada aplicación y extensión que utiliza esa persona y absolutamente *todo* su historial de YouTube.[30] Por su parte, Facebook recolecta datos sobre las personas incluso si no tienen una cuenta de Facebook.[31]

En un principio, cualquier dato que se creara como consecuencia del suministro del servicio de Internet era considerado un "escape de datos". El descubrimiento de que ese dato en realidad revelaba información significativa sobre el comportamiento de las personas, y por ende podía monetizarse, fue un paso clave en el desarrollo del modelo de negocios basado en la vigilancia que usan Google y Facebook.[32] A este hallazgo le siguió la rápida reducción del costo de almacenamiento de los datos, con lo que las empresas adquirieron la capacidad de expandir sus bóvedas de datos de manera habitual.[33]

Por otra parte, el modelo de negocios basado en la vigilancia de Google y Facebook también podría fomentar la "datificación", es decir, plasmar en forma de datos muchos aspectos del mundo que nunca antes se habían cuantificado.[34] A propósito de ello, el seguimiento ha comenzado a incluir el mundo físico, a medida que la expansión de la "Internet de las cosas"[35] crea un mundo analógico minado de sensores de ambiente. Por ejemplo, dentro del hogar de una persona, es posible encontrar asistentes domésticos

28. Kashmir Hill, *Goodbye Big Five*, Gizmodo, enero de 2019, https://gizmodo.com/c/goodbye-big-five

29. En la respuesta de Facebook (ver el anexo que se incluye), se señala que la única información personal que las personas deben proporcionar para registrarse en Facebook es su "nombre, edad, género e información de contacto". Sin embargo, Facebook también recopila una gran cantidad de datos sobre los usuarios después de que estos se registran, por ejemplo, el contenido de la información que comparten en Facebook, información sobre las personas con las que están conectados o con quienes interactúan e información sobre la actividad de las personas en la plataforma. Ver la Política de datos de Facebook: https://www.facebook.com/policy.php

30. Dylan Curran, Guardian, *Are you ready? Here is all the data Facebook and Google have on you,* marzo de 2018

31. Facebook, *Hard Questions: What Data Does Facebook Collect When I'm Not Using Facebook, and Why?*, abril de 2018, https://newsroom.fb.com/news/2018/04/data-off-facebook. Facebook señala que no crea perfiles de personas que no sean usuarios (ver el anexo que se incluye).

32. Zuboff cita una patente presentada por Google en 2003 para ilustrar el cambio de foco de la empresa hacia un modelo de contenido dirigido según el comportamiento. La patente establece que "el presente invento podría implicar nuevos métodos, sistemas, formatos de mensaje o estructuras de datos para determinar información del perfil de los usuarios y utilizar dicha información específica de los usuarios con fines de publicidad". Shoshana Zuboff, *How Google Discovered the Value of Surveillance*, 2019 https://longreads.com/2019/09/05/how-google-discovered-the-value-of-surveillance/

33. Schneier 2015, p. 27

34. Kenneth Neil Cukier y Viktor Mayer-Schoenberger, *The Rise of Big Data: How It's Changing the Way We Think About the World,* Foreign Affairs, mayo/junio de 2013, https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data

35. El concepto de "Internet de las cosas" puede describirse como una red en expansión de dispositivos conectados a través de Internet, desde refrigeradores hasta sistemas de calefacción inteligentes de manera que estos aparatos pueden comunicarse entre sí y con los usuarios, desarrolladores y aplicaciones, gracias a la recopilación y el intercambio de datos de su entorno monitoreado.

como el Asistente de Google y Portal de Facebook, así como sistemas domésticos inteligentes que conectan múltiples dispositivos como teléfonos, televisores y sistemas de calefacción.[36] La extracción de datos abarca cada vez más aspectos de los espacios públicos mediante la infraestructura de las "ciudades inteligentes" diseñadas para recolectar datos en toda una área urbana.[37] De hecho, Facebook está en vías de desarrollar una tecnología que permitiría rastrear los procesos que tienen lugar dentro del cerebro humano.[38]

Asimismo, las empresas buscan expandirse a nuevos mercados internacionales (ver cuadro abajo). El ejemplo más evidente lo aporta Free Basics, el servicio de Internet "gratuito" de Facebook para el que el gigante se ha aliado con operadores de telefonía móvil en más de 65 países a fin de atraer a las personas al mundo en línea. En muchos países del Sur Global, Free Basics es directamente la opción de Internet.[39] Un ejemplo de la iniciativa de expansión de Google es el proyecto "Dragonfly", el intento de la empresa de volver a ingresar en el mercado chino de motores de búsqueda para acceder a datos de más de 800 millones de usuarios de Internet.[40] Fue un intento fallido, ya que sus mismos empleados y grupos de activistas de los derechos humanos obligaron a la empresa a poner fin al programa.[41]

Google y Facebook también se están expandiendo hacia nuevas áreas que amplían el alcance de su proceso de recolección de datos. Actualmente, Facebook lidera la creación de Libra, una nueva criptomoneda global. Esta decisión hizo que un grupo de autoridades reguladoras de protección de datos de distintas partes del

RECOPILACIÓN DE DATOS EN EL SUR GLOBAL

Tanto Facebook como Google han buscado ampliar su alcance en los países en desarrollo del Sur Global.[42] Los mercados emergentes representan oportunidades lucrativas de crecimiento para Facebook y Google, en gran medida debido al potencial de aumentar el acceso a los datos.

El servicio Free Basics es otra de las formas que usa Facebook para recolectar enormes cantidades de datos de las personas en países en desarrollo. Según un informe reciente de las Naciones Unidas: "Para las plataformas de anuncios, como Google y Facebook, contar con más datos (locales) podría abrir nuevas oportunidades para brindar mejores anuncios dirigidos... Con Free Basics de Facebook, el tráfico se redirige a través de un portal, lo que da cuenta de la dependencia del modelo de negocios de Facebook de una plataforma más cerrada".[43]

Según su respuesta a este informe (ver anexo), Facebook sostiene que "Free Basics no almacena información sobre las cosas que las personas hacen o sobre el contenido que ven en cualquier aplicación de terceros". Sin embargo, de acuerdo con la Política de Privacidad de Free Basics, el servicio sí recopila datos sobre el uso de servicios de terceros para ofrecer servicios más personalizados y también almacena información sobre los servicios a los que se ha accedido, junto con el número de teléfono de los usuarios, durante noventa días.[44] Aunque Facebook presenta Free Basics como una iniciativa filantrópica que equivale a una "vía hacia una Internet más

36. CNet, *Google calls Nest's hidden microphone an 'error'*, febrero de 2019

37. Otra empresa que tiene como objetivo vigilar el mundo físico es Sidewalk Labs, también subsidiaria de Alphabet, que se dedica al diseño de soluciones tecnológicas para "ciudades inteligentes" y las proporciona a municipios. Ver Ellen P. Goodman, Julia Powles, *Urbanism Under Google: Lessons from Sidewalk Toronto*, Fordham Law Review, mayo de 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3390610

38. TechCrunch, *Facebook is exploring brain control for AR wearables*, julio de 2019 https://techcrunch.com/2019/07/30/facebook-is-exploring-brain-control-for-ar-wearables/

39. Es muy probable que quienes viven en países en vías de desarrollo y pueden pagar por el servicio de Internet utilicen un teléfono con sistema Android, lo que significa que esas personas también están siendo vigiladas por Google.

40. China Internet Watch, *China internet users snapshot 2019*, abril de 2019, citando la cantidad de usuarios de Internet en China a diciembre de 2018. De acuerdo con las filtraciones de los comentarios del Vicepresidente de Búsquedas de Google, Ben Gomes, el proyecto Dragonfly formaba parte de la iniciativa "*Next Billion Users*" para expandir su base de usuarios a nivel global. Ver Ryan Gallagher, *Leaked Transcript Of Private Meeting Contradicts Google's Official Story On China*, The Intercept, 9 de octubre de 2018

41. Amnistía Internacional, *Google must fully commit to never censor search in China*, julio de 2019

42. Wired, *Facebook and Google's race to connect the world is heating up*, 26 de julio de 2018, https://www.wired.co.uk/article/google-project-loon-balloon-facebook-aquila-internet-africa

43. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, *Digital Economy Report 2019 (Informe sobre la economía digital 2019)*, septiembre de 2019, en: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

44. Facebook, *Privacy on Free Basics*, en: https://www.facebook.com/legal/internet.org_fbsterms. Según la política: "Para que este proceso funcione, recibimos y almacenamos cierta información limitada: el dominio o el nombre del Servicio de terceros al cual se obtiene acceso a través de Free Basics, y la cantidad de datos (p. ej., megabytes) utilizados al acceder o usar dicho servicio. Esta información también nos ayuda a mejorar y personalizar tu experiencia con Free Basics, puesto que nos permite mostrarte los servicios que más utilizas para facilitarte el acceso. Almacenamos estos datos junto con tu número de teléfono solo por 90 días. Una vez transcurrido este período, la información se procesa como datos globales o bien se anonimiza de algún otro modo".

generalizada" para las personas en el Sur Global que, de otra forma, no tendrían acceso a la web, el servicio más bien parece una "vía" para incrementar la minería de datos en estos países.[45]

Una investigación de Privacy International identificó que un teléfono celular de bajo costo producido para el mercado filipino y con sistema operativo Android carecía del nivel de seguridad adecuado, sobre todo a causa de las aplicaciones instaladas por el fabricante, que exponían los datos de los usuarios a riesgos de explotación por parte de estafadores, partidos políticos y organismos gubernamentales.[46] Los usuarios del Sur Global, para quienes los dispositivos más económicos pueden ser la única forma de acceder a Internet, son potencialmente aún más vulnerables ante las prácticas de vigilancia masiva y explotación de los datos.

mundo planteara preocupaciones respecto de la privacidad y el hecho de combinar enormes reservas de información personal con información financiera.[47] Mientras tanto, el acceso de Google a datos de pacientes del Servicio Nacional de Salud (NHS) del Reino Unido, primero a través de su subsidiaria DeepMind y ahora directamente por medio de su división de Salud, ha sido una constante fuente de controversia frente al riesgo de que esos datos se fusionen con las bóvedas de datos de Google.[48] Además, recientemente, Google adquirió Fitbit, una empresa de seguimiento del estado físico, lo que le da acceso a una de las bases de datos de actividad, ejercicio y sueño más grandes del mundo.[49]

La iniciativa de ampliar las bóvedas de datos también incentiva a las empresas a fusionar y combinar datos de sus distintas plataformas, lo que a su vez acrecienta el poder y la hegemonía de cada plataforma individual. En 2012, Google implementó un cambio radical en su política de privacidad que le permitía a la empresa combinar datos de todos sus servicios. Esto le valió el rechazo de los defensores de la privacidad y las autoridades reguladoras.[50] Asimismo, cuando Facebook adquirió WhatsApp en 2014, hizo declaraciones en las que aseguraba que mantendría los servicios funcionando por separado. Sin embargo, en 2016, la empresa adoptó un polémico cambio en su política de privacidad que le permitía compartir datos entre los dos servicios, incluso para fines publicitarios.[51] Debido a investigaciones posteriores realizadas por autoridades regulatorias europeas, Facebook y WhatsApp se vieron obligados a revertir el intercambio de datos entre los dos servicios en la Unión Europea.[52] Según se informa, Facebook planea integrar Facebook, Messenger, Instagram y WhatsApp aún más en el futuro, pero la empresa señala que esto no le permitirá a la empresa agrupar más datos sobre las personas.[53]

45. Facebook Free Basics https://connectivity.fb.com/free-basics/

46. Privacy International, *"Buying a smart phone on the cheap? Privacy might be the price you have to pay"*, 20 de septiembre de 2019, https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay

47. *Joint statement on global privacy expectations of the Libra network*, 5 de agosto de 2019 https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf

48. Natasha Lomas, *Google gobbling DeepMind's health app might be the trust shock we need*, TechCrunch, noviembre de 2018, https://techcrunch.com/2018/11/14/google-gobbling-deepminds-health-app-might-be-the-trust-shock-we-need/. Google afirma que los fideicomisos del NHS se encuentran "en pleno control de todos los datos de los pacientes, y nosotros solo utilizaremos los datos de los pacientes para ayudar a mejorar la atención, bajo su supervisión y de acuerdo con sus instrucciones". https://www.blog.google/technology/health/deepmind-health-joins-google-health/

49. Fitbit, *Fitbit to Be Acquired by Google*, 1 de noviembre de 2019, https://investor.fitbit.com/press/press-releases/press-release-details/2019/Fitbit-to-Be-Acquired-by-Google/default.aspx

50. The Verge, *Google's 2012 privacy policy changes: the backlash and response*, febrero de 2012, https://www.theverge.com/2012/2/1/2763898/google-privacy-policy-changes-terms-of-service-2012

51. Natasha Lomas, *WhatsApp to share user data with Facebook for ad targeting — here's how to opt out*, TechCrunch, agosto de 2016 https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/

52. Oficina del Comisionado de Información del Reino Unido, *A win for the data protection of UK consumers*, marzo de 2018, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/blog-a-win-for-the-data-protection-of-uk-consumers/

53. Mike Isaac, *Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger*, New York Times, 25 de enero de 2019, https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html ; Ver carta de Facebook a Amnistía Internacional en el anexo que se incluye.

VIGILANCIA OMNIPRESENTE

La naturaleza masiva de la recolección de datos en Internet ha sido descrita por el experto en ciberseguridad Bruce Schneier como "vigilancia omnipresente".[54] En la práctica, esto significa que las personas están siendo rastreadas constantemente cuando usan Internet todos los días y cada vez más también en el mundo analógico.

La vigilancia va mucho más allá de la información que brindan los usuarios cuando interactúan con Google y Facebook, como su dirección de correo electrónico, fecha de nacimiento y número de teléfono; además, incluye su ubicación, historial de búsqueda y uso de aplicaciones.

Google y Facebook son los principales agentes de rastreo de las actividades de navegación en línea, lo que incluye las búsquedas que hacen las personas, los sitios web que visitan y desde qué ubicación lo hacen. Por ejemplo, Google recopila datos mediante un sistema de rastreo incorporado en el navegador Chrome y el sistema operativo Android, a través de todos los sitios que usan Google Analytics, y también por medio de AdSense, su software de publicidad omnipresente. Según lo que se conocía, el rastreo de datos de Facebook se producía cuando alguien visitaba un sitio web con un *plugin* de Facebook, como los botones "Me gusta" o "Compartir", o una parte de código oculto, conocido como el píxel de Facebook. En 2018, Facebook afirmó que "el botón 'Me gusta' aparecía en 8,4 millones de sitios web; el botón 'Compartir' figuraba en 931.000 páginas web, y había 2,2 millones de píxeles de Facebook instalados en diferentes sitios de Internet"; y Facebook recibe información cuando alguien visita uno de estos sitios.[55]

En la respuesta de Facebook a este informe (ver anexo), se aclara que "excepto por motivos de seguridad y para protección contra fraude, Facebook ya no almacena datos de *plugins* sociales (p. ej., el botón "Me gusta") con identificadores del usuario o el dispositivo". Sin embargo, en la Política de datos de Facebook, se aclara que la empresa, por lo menos, todavía recibe esos datos: "Los anunciantes, los desarrolladores de apps y los editores pueden enviarnos información por medio de las herramientas empresariales de Facebook que usan, incluidos nuestros *plugins* sociales... Estos socios nos brindan información sobre las actividades que realizas fuera de Facebook... ya sea que tengas o no una cuenta de Facebook o hayas iniciado sesión en ella".[56]

El *smartphone* constituye el principal dispositivo que utilizan las personas para conectarse a Internet y, por consiguiente, es una rica fuente de datos, que incluyen datos de ubicación y datos provenientes de todas las aplicaciones y servicios que ofrece el teléfono, entre otros.[57] La gran mayoría de los *smartphones* utilizan el sistema operativo Android de Google. Según los resultados de un estudio, un celular con Android que no estaba en uso envió 900 puntos de datos a Google en el transcurso de 24 horas, incluidos datos de ubicación.[58] Sensorvault, la base de datos de Google para datos de ubicación de teléfonos con Android, contiene "registros detallados de ubicación con datos de al menos cientos de millones de dispositivos de todo el mundo que datan de hace casi una década".[59] Facebook también rastrea los datos de los usuarios de Android a través de sus aplicaciones, por ejemplo, el registro de llamadas de las personas y su historial de SMS, aunque la empresa ha señalado que solo lo hace si tiene el consentimiento del usuario.[60]

54. Schneier 2015, p. 38

55. Rebecca Stimson, Gerenta de Políticas Públicas, Facebook en el Reino Unido, *Letter to Chair of UK House of Commons Digital, Culture, Media and Sport Committee*, 14 de mayo de 2018, p. 2 https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/180514-Rebecca-Stimson-Facebook-to-Ctte-Chair-re-oral-ev-follow-up.pdf

56. Política de datos de Facebook: https://www.facebook.com/policy.php. Además, la Política de cookies de Facebook señala que "Podemos colocar cookies en tu computadora o dispositivo, y recibir información almacenada en ellas cuando utilizas o visitas... Los sitios web y las aplicaciones proporcionados por otras empresas que utilizan los Productos de Facebook... Facebook usa cookies y recibe información cuando visitas esos sitios y aplicaciones, incluida información sobre dispositivos e información sobre tu actividad, sin ninguna intervención adicional de tu parte. Esto sucede sin importar si tienes o no una cuenta de Facebook o si iniciaste sesión en ella". https://www.facebook.com/policies/cookies

57. World Advertising Research Center (WARC), *Almost three quarters of internet users will be mobile-only by 2025*, enero de 2019; Un estudio del New York Times sobre el seguimiento de la ubicación de los *smartphones* reveló que hay una cantidad exhaustiva de datos de ubicación privados a la venta. *Ver Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, 10 de diciembre de 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

58. Profesor Douglas C. Schmidt, Vanderbilt University, *Google Data Collection*, Digital Content Next, agosto de 2018, párrafo 24 https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

59. Según los empleados de Google citados en The New York Times, *Tracking Phones, Google Is a Dragnet for the Police*, abril de 2019 https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

60. Comité de Tecnología Digital, Cultura, Medios y Deportes de la Cámara de los Comunes del Reino Unido, *Final Report on Disinformation and 'fake news'*, febrero de 2019, p. 35; Facebook, *Fact Check: Your Call and SMS History*, 25 de marzo de 2018 https://newsroom.fb.com/news/2018/03/fact-check-your-call-and-sms-history/

Asimismo, hay otras aplicaciones de Android que también comparten datos con Facebook.[61]

Es importante destacar que la información que recopilan Facebook y Google abarca no solo datos en sí, sino también metadatos, o "datos sobre los datos". Esto incluye, por ejemplo, los destinatarios de los mensajes de correo electrónico, registros de ubicación y la fecha y hora de los correos electrónicos y las fotos. El uso cada vez más generalizado del cifrado de extremo a extremo para los mensajes, por ejemplo, en WhatsApp, implica que, hoy en día, incluso las mismas empresas suelen no tener acceso al contenido de las comunicaciones. No obstante, no es novedad que los metadatos constituyen "información que no es menos sensible —si se tiene en cuenta el derecho a la privacidad— que el contenido de las comunicaciones en sí".[62] La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) ha reconocido que, al analizarlos y combinarlos, los metadatos "pueden dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada".[63]

Además, si bien el contenido de los datos es muy revelador cuando se hacen acciones dirigidas a una persona o a un pequeño grupo de personas, cuando se recolectan al nivel de Facebook y Google, los metadatos son mucho más valiosos. Esto es así porque la analítica compleja es capaz de predecir patrones de comportamiento a escala poblacional[64] y se puede usar potencialmente para inferir información confidencial sobre las personas, como su identidad sexual, sus opiniones políticas, sus rasgos de personalidad u su orientación sexual, todo mediante modelos algorítmicos sofisticados.[65] Estas intromisiones se pueden realizar independientemente de los datos que proporcione el usuario y a menudo controlan la manera en que las personas son vistas y evaluadas por terceros: por ejemplo, se sabe que hay terceros que anteriormente han utilizado esos datos para controlar quién ve anuncios de alquiler[66] y determinar la elegibilidad de ciertas personas para acceder a un préstamo.[67]

61. Privacy International, *How Apps on Android Share Data with Facebook*, diciembre de 2018. En el estudio, el 61 % de las aplicaciones probadas automáticamente transfería datos a Facebook cuando el usuario abría la aplicación. Posteriormente, algunas de esas aplicaciones dejaron de hacerlo. https://privacyinternational.org/appdata

62. *Tele2 Sverige AB* y C-698/15 *Watson y otros* (ECLI:EU:C:2016:970) (*"Watson"*) Tribunal de Justicia de la Unión Europea, asuntos acumulados C-203/15 en el párrafo 99, http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

63. Informe del ACNUDH sobre el derecho a la privacidad en la era digital, 30 de junio de 2014, A/HRC/27/37, párrafo 19.

64. De ahí que WhatsApp tenga un valor inconmensurable. A diferencia de las otras plataformas de Facebook, WhatsApp no contiene anuncios. Además, gracias al cifrado de extremo a extremo, Facebook no puede acceder al contenido de los mensajes que circulan por la plataforma, aunque WhatsApp suministra una inmensa cantidad de datos a Facebook: por ejemplo, información sobre la ubicación de los usuarios, listas de contacto y metadatos correspondientes a más de 65.000 millones de mensajes diarios.

65. Privacy International, *Examples of Data Points Used in Profiling*, abril de 2018, https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf; Facebook señala que no infiere la identidad sexual, rasgos de personalidad u orientación sexual de las personas. Ver el anexo que se incluye.

66. Julia Angwin, Ariana Tobin y Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, ProPublica, noviembre de 2017. En marzo de 2019, Facebook anunció que aplicaría restricciones a las opciones de segmentación de anuncios de viviendas, empleo y crédito en los EE. UU., después de llegar a un acuerdo con organizaciones de derechos civiles.

67. Astra Taylor y Jathan Sadowski, How Companies Turn Your Facebook Activity Into a Credit Score, The Nation, mayo de 2015, https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/

LAS EMPRESAS Y LOS DERECHOS HUMANOS

De acuerdo con las normas internacionales sobre derechos humanos, los Estados son los principales garantes de estos derechos y tienen el deber de proteger a los ciudadanos contra las violaciones de derechos por parte de las empresas y otros terceros. El Consejo de Derechos Humanos de las Naciones Unidas ha afirmado que los mismos derechos que tienen las personas en el mundo analógico deben protegerse también en Internet, y que los Estados deben crear y mantener un "entorno en línea propicio" para el ejercicio de los derechos humanos.[68]

Todas las empresas tienen la responsabilidad de respetar todos los derechos humanos independientemente de la capacidad o la voluntad de los Estados de cumplir con sus obligaciones en materia de derechos humanos, e incluso más allá del cumplimiento de las leyes y regulaciones nacionales.[68] Las normas relativas a las empresas y los derechos humanos, como los Principios Rectores sobre las Empresas y los Derechos Humanos de la ONU, establecen "norma[s] de conducta mundial" aplicables a todas las empresas, donde sea que operen.[70]

En el marco del cumplimiento de su responsabilidad, las empresas deben asumir en sus políticas el compromiso de respetar los derechos humanos y adoptar medidas constantes, proactivas y reactivas para asegurarse de no causar violaciones de tales derechos ni contribuir a ellas, proceso que se denomina "diligencia debida en materia de derechos humanos". La diligencia debida en materia de derechos humanos exige a las empresas que identifiquen los impactos respecto de los derechos humanos asociados con sus operaciones (tanto potenciales como actuales), que tomen medidas efectivas para prevenir y mitigar dichos impactos y que sean transparentes al rendir cuentas sobre sus esfuerzos respecto de este tema. Esto incluye abordar los altos niveles de riesgo de impacto negativo sobre los derechos humanos que prevalecen dentro de un determinado sector por las características propias de esa área.[71]

68. Consejo de Derechos Humanos de la ONU, *Promoción, protección y disfrute de los derechos humanos en Internet*, julio de 2018, documento A/HRC/38/L.10/Rev.1

69. Principios rectores sobre las empresas y los derechos humanos de las Naciones Unidas: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar", 2011, documento HR/PUB/11/04, (Principios rectores) www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

70. Principios rectores, principio rector 11

71. Guía de la OCDE de debida diligencia para una conducta empresarial responsable, sección II, 2.1, Pregunta 22 del anexo

2. ATAQUE A LA PRIVACIDAD

"Sabemos dónde estás. Sabemos dónde has estado. Podemos llegar a saber en qué estás pensando".

Eric Schmidt, ex CEO de Google, 2010[72]

Por años, los defensores de la privacidad han criticado abiertamente a Google y Facebook y, durante las dos últimas décadas, ambas empresas se han visto inmersas en varios escándalos relacionados con la forma en la que utilizan los datos personales. No obstante, ninguna de las dos ha dejado de ampliar el alcance y la profundidad de la extracción y el tratamiento de los datos que llevan a cabo. Esto ha dado origen a la actual arquitectura de vigilancia descrita en la sección anterior.

72. The Atlantic, *Google's CEO: 'The Laws Are Written by Lobbyists'*, octubre de 2010, https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/

En 2010, el CEO de Facebook, Mark Zuckerberg, pronunció la famosa frase respecto de que las redes sociales habían cambiado la privacidad entendida "como norma social".[73] De hecho, el aumento de las tecnologías digitales ha hecho que la privacidad sea un derecho aún más importante hoy en día. Sin embargo, el modelo de negocios de Google y Facebook perjudica la esencia misma del derecho a la privacidad.

Facebook ha dejado claro que está "totalmente en desacuerdo" con la idea de que su modelo de negocios es un modelo "basado en la vigilancia" y argumenta que el uso de sus productos es completamente voluntario y, por lo tanto, es diferente a la vigilancia gubernamental involuntaria en virtud de lo contemplado por el derecho a la privacidad.[74] Sin embargo, en el derecho internacional de derechos humanos, se reconoce ampliamente que el derecho a la privacidad debe estar garantizado respecto de interferencias arbitrarias "ya sea que provengan de las autoridades estatales o de personas físicas o jurídicas (como las corporaciones)".[75] Este capítulo explica de qué manera las actividades actuales de Google y Facebook son fundamentalmente incompatibles con este derecho.

EL MODELO DE NEGOCIOS BASADO EN LA VIGILANCIA Y EL DERECHO A LA PRIVACIDAD

El derecho a la privacidad contempla que ninguna persona debe ser objeto de "injerencias arbitrarias o ilegales" en su vida privada, su familia, su domicilio o su correspondencia y que toda persona tiene derecho a la protección de la ley contra esas injerencias.[76] Hace tiempo que el Comité de Derechos Humanos de la ONU ha reconocido que dicha protección incluye la regulación de "la recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas".[77]

El alcance del derecho a la privacidad ha evolucionado constantemente en respuesta a los cambios sociales, en especial ante los nuevos avances tecnológicos. El ACNUDH ha establecido que "la privacidad puede entenderse como la presunción de que el individuo debe tener una esfera de desarrollo autónomo, interacción y libertad, una "esfera privada" con o sin relación con otras y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados".[78] Esto abarca tres conceptos interrelacionados: la libertad de protegernos contra la intromisión en nuestra vida privada, el derecho a controlar la información sobre nuestra persona, y el derecho a disponer de un espacio en el que podamos expresar nuestra identidad libremente. La naturaleza del modelo de negocios de Google y Facebook basado en la vigilancia omnipresente socava cada uno de esos tres elementos, a tal punto que ha menoscabado la mismísima esencia de la privacidad.

El ACNUDH ha reconocido que "el simple hecho de que se generen y reúnan datos relativos a la identidad, la familia o la vida de una persona ya afecta a su derecho a la privacidad, pues a través de esas acciones, la persona pierde en cierta medida el control sobre una información que podría poner en riesgo su vida privada".[79] La magnitud de los datos recopilados por Google y Facebook implica que estas empresas están recabando más información sobre los seres humanos de lo que antes podíamos imaginar. La acumulación de semejante cantidad de datos, junto con el uso de herramientas

73. Ann Cavoukian, ex Comisionada de Información y Privacidad de Ontario, *Privacy is still a social norm*, The Globe and Mail, marzo de 2010 https://www.theglobeandmail.com/opinion/privacy-is-still-a-social-norm/article1209523/

74. Carta de Facebook a Amnistía Internacional, noviembre de 2019. Ver el anexo que se incluye.

75. Comité de Derechos Humanos de las Naciones Unidas, Observación general del CCPR núm. 16, HRI/GEN/1/Rev.9 (Vol. I), 1988, párrafo 1. Además, los principios rectores sobre las empresas y los derechos humanos de las Naciones Unidas indican claramente que las empresas tienen la responsabilidad de respetar "todo el espectro de los derechos humanos internacionalmente reconocidos" (principio rector 12).

76. Declaración Universal de los Derechos Humanos, art. 12; Pacto Internacional de Derechos Civiles y Políticos, art. 17.

77. Comité de Derechos Humanos de las Naciones Unidas, Observación general del CCPR núm. 16: art. 17 (derecho a la privacidad), el derecho al respeto de la vida privada, la familia, el domicilio y la correspondencia, y la protección de la honra y la reputación, 8 de abril de 1988, https://www.refworld.org/docid/453883f922.html

78. Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *El derecho a la Privacidad en la Era Digital*, 3 de agosto de 2018, A/HRC/39/29, párrafo 5.

79. A/HRC/39/29, párrafo 7; véase también A/HRC/27/37, párrafo 20, y Tribunal Europeo de Derechos Humanos, *Weber y Saravia c. Alemania,* párrafo 78; *Malone c. el Reino Unido,* párrafo 64.

de análisis de datos sofisticadas, puede revelar información muy íntima y detallada; en efecto, estas empresas pueden saber prácticamente todo acerca de una persona.[80]

La injerencia en el derecho de una persona a la privacidad solo está permitida en virtud de las normas internacionales de derechos humanos siempre que no sea ni arbitraria ni ilegal. Los mecanismos de protección de los derechos humanos siempre han interpretado esas palabras bajo la luz de los principios generales de legalidad, necesidad y proporcionalidad.[81] La vigilancia corporativa indiscriminada a semejante escala es inherentemente innecesaria y desproporcionada y jamás puede ser una injerencia permisible en el derecho a la privacidad. A modo de comparación, en los casos en que los Estados han indicado que la vigilancia masiva e indiscriminada era necesaria para proteger la seguridad nacional, los mecanismos de protección de los derechos humanos han afirmado que esta práctica "no es permisible en virtud del derecho internacional de los derechos humanos, ya que no sería posible realizar un análisis individualizado de la necesidad y la proporcionalidad en el contexto de esas medidas".[82]

El segundo componente del derecho a la privacidad contempla que las personas tienen derecho a controlar su información personal, o derecho a la "autodeterminación informativa"[83], es decir, a ser capaces de decidir cuándo y cómo se pueden compartir nuestros datos personales con terceros.[84] Este es el fundamento de la protección de los datos, que se ha vuelto un asunto cada vez más importante desde el auge de las bases de datos de gran volumen y los avances de la tecnología informática. El Tribunal Europeo de Derechos Humanos ha reconocido que la protección de los datos personales es de vital importancia para que las personas puedan ejercer plenamente su derecho a la privacidad[85], y que la privacidad habilita el derecho a una forma de autodeterminación informativa.[86] El modelo de negocios basado en la vigilancia entra en conflicto directo con los principios fundamentales que sostienen este segundo componente y, por lo tanto, socava la capacidad de las personas de ejercer control sobre su información personal, lo que incluye tener la libertad de elegir las formas en que se utilizan sus datos personales y con qué motivo (ver recuadro a continuación).

PROTECCIÓN DE DATOS

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que entró en vigor en mayo de 2018, se ha convertido en el marco de referencia mundial en materia de protección de datos y regulación de la privacidad. Google y Facebook son empresas obligadas en el marco del RGPD, que se aplica a todas las organizaciones ubicadas en la UE y también a aquellas fuera de la UE que ofrecen servicios a personas que se encuentran en la UE o que monitorean el comportamiento de estas personas.

Es importante resaltar que el reglamento define "datos personales" en términos generales como "toda información sobre una persona física identificada o identificable".[87] La definición incluye datos relacionados con toda persona cuya identidad pueda determinarse, directa

80. Privacy International, *A Snapshot of Corporate Profiling*, abril de 2018, https://privacyinternational.org/long-read/1721/snapshot-corporate-profiling

81. A/HRC/27/37, párrafos 21-27.

82. Informe del ACNUDH relativo a las mejores prácticas y lecciones extraídas sobre cómo la protección y la promoción de los derechos humanos contribuyen a la prevención y erradicación del extremismo violento, 21 de julio de 2016, A/HRC/33/29, párrafo 58; véase también el Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, 23 de septiembre de 2014, A/69/397, párrafo 47, y A/HRC/27/37, párrafo 25.

83. El término "autodeterminación informativa" se utilizó por primera vez en el contexto de un fallo constitucional alemán respecto de la recopilación de información personal durante el censo de 1983: Bundesverfassungsgericht [BVerfG], 15 de diciembre de 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1. El Tribunal entendió el término como el poder que tiene cada persona de decidir cuándo y dentro de qué parámetros se puede comunicar la información sobre su vida privada a otras personas.

84. Alan Westin, Privacy and Freedom, 1967

85. *S y Marper c. el Reino Unido,* demandas nro. 30562/04 y 30566/04, Tribunal Europeo de Derechos Humanos (TEDH), 4 de diciembre de 2008, disponible en http://hudoc.echr.coe.int/eng?i=001-90051.

86. Satakunnan Markkinapörssi Oy y Satamedia Oy c. Finlandia, 931/13, TEDH, 27 de junio de 2017, párrafo 137, disponible en https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175121%22]}.

87. RGPD, art. 4(1).

o indirectamente, a partir de los datos en cuestión.[88] El RGPD deja en claro que los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable.[89] Asimismo, los datos que se infieren y se predicen se consideran "datos personales" si se encuentran vinculados a identificadores únicos o si de algún modo pueden atribuirse a una persona física identificable.

Uno de los principios clave del RGPD es el de "limitación de la finalidad", que exige a las empresas que recopilan y procesan datos personales que sean claras respecto de la finalidad del tratamiento de esos datos desde el comienzo. Además, también les exige que registren la finalidad del tratamiento y que la especifiquen en la política de privacidad que ponen a disposición de las personas. Por último, según este principio, si las empresas quieren utilizar los datos personales con una finalidad distinta, es necesario que este tratamiento sea compatible con el fin original, que la persona en cuestión otorgue su consentimiento, o bien que las empresas tengan otra base jurídica clara.[90]

El RGPD también establece un elevado estándar en lo que respecta al consentimiento, que se define como toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernen.[91] Si el tratamiento tiene varias finalidades diferentes, el RGPD indica con claridad que se deberá contar con el consentimiento de la persona para cada una de ellas[92]. El reglamento también determina que para asegurar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento.[93] En contraposición con el requisito de que el consentimiento debe darse libremente, el modelo de negocios basado en la vigilancia recurre a servicios sujetos a la condición de que las personas otorguen su consentimiento para el tratamiento y el intercambio de sus datos personales con fines de marketing y publicidad, lo que significa que los sujetos no pueden negar o revocar su consentimiento sin quedar expulsados de estos espacios como consecuencia.[94]

Por último, existe un consenso generalizado respecto de que la privacidad también es imprescindible para crear y proteger el espacio necesario para construir nuestras propias identidades.[93] El Comité de Derechos Humanos de las Naciones Unidas (CCPR) ha definido la privacidad como "la esfera de la vida de una persona en la que esta puede expresar libremente su identidad".[96] De esta definición se desprende que nuestro sentido de la identidad se construye en sociedad y es dinámico: según el contexto, mostramos una u otra cara de nuestra persona, ya sea con nuestros amigos, en el trabajo o en público, y tales identidades están en permanente proceso de cambio y adaptación. La privacidad nos permite decidir por nosotros mismos de qué forma queremos que nos vean los demás, y, de hecho, nos comportamos de manera diferente cuando estamos ante la observación no deseada de terceros. En este sentido, la privacidad resulta imprescindible para nuestra autonomía y capacidad de determinar nuestra propia identidad.

88. *Ibid.*

89. RGPD, considerando 26

90. Ver RGPD, arts. 5(1)(b), 6(4) y 30, y considerandos 39 y 50.

91. RGPD, art. 4(11).

92. Ver RGPD, arts. 6(1)(a), 7 y considerando 32.

93. RGPD, considerando 43

94. Dicho "consentimiento forzado" fue impugnado en virtud del Reglamento General de Protección de Datos de la UE en el marco de una acción iniciada por la organización por los derechos del consumidor Noyb en contra de Google y Facebook: https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.

95. Ver, por ejemplo, Agre y Rotenburg (eds), *Technology and Privacy: The New Landscape*, 1998; Julie E. Cohen, 2013

96. Comité de DD. HH., *Coeriel y Aurik c. los Países Bajos* (1994), comunicación n.º 1991, párrafo 10.2

Las personas que se encuentran bajo vigilancia constante están sometidas a adaptarse bajo presión. El papel fundamental de la privacidad a la hora de dar lugar a distintas identidades fomenta la diversidad cultural. Muchas veces la superposición de identidades constituye la condición básica de una minoría que busca vivir, trabajar y subsistir en el seno de una cultura dominante. Por ejemplo, ese podría ser el caso de un grupo de personas del colectivo LGBTI que viven en una cultura en la que las conductas íntimas entre personas del mismo sexo son estigmatizadas o ilegales; lo mismo podría sucederles a integrantes del colectivo LGBTI que no viven en esas culturas, pero tienen familiares que sí.[97] También podría ser el caso de alguien que participa en una parte vulnerable de la economía informal, como el trabajo sexual.[98]

La tremenda magnitud de la injerencia del modelo de negocios de Google y Facebook en nuestra vida privada a través de la vigilancia omnipresente y constante ha reducido enormemente el espacio necesario para que podamos definir quiénes somos. La privacidad nos protege contra "los esfuerzos de los actores comerciales y gubernamentales de hacer que las personas y las comunidades se vuelvan estáticas, transparentes y predecibles".[99] En cambio, la verdadera naturaleza de la segmentación, que consiste en usar datos para inferir características detalladas sobre las personas, implica que Google y Facebook están definiendo nuestra identidad ante el mundo exterior, a menudo en una gran cantidad de contextos que afectan a los derechos humanos. Este mecanismo invade nuestra vida privada y contradice directamente nuestro derecho a la autodeterminación informativa y a definir nuestras propias identidades en una esfera de privacidad.

En pocas palabras, la vigilancia a tan gran escala representa una injerencia nunca antes vista en el derecho a la privacidad, de modo que no puede ser compatible con la responsabilidad de las empresas de respetar los derechos humanos. Esto va más allá de la intromisión en cada aspecto de nuestra vida en Internet y, de hecho, atenta contra nuestro derecho de determinar y definir quiénes somos como sujetos autónomos en la sociedad.

LAS PROMESAS QUE SE HICIERON SOBRE LA PRIVACIDAD Y LOS INTENTOS FALLIDOS DE RESPETARLA

Hace poco, los ejecutivos al mando de Google y Facebook hicieron declaraciones públicas en las que reconocieron el derecho a la privacidad. En mayo, el CEO de Google, Sundar Pichai, publicó un artículo de opinión sobre la privacidad.[100] En marzo, el CEO de Facebook, Mark Zuckerberg, anunció que Facebook haría un cambio con miras a la privacidad[101], y en mayo dio su conferencia anual junto a una pantalla con la leyenda "El futuro es privado".[102]

En este contexto, ambas empresas han anunciado que implementarán nuevas medidas con el objetivo de darles a los usuarios de sus plataformas más control de su privacidad.[103] En noviembre, Google anunció que implementaría mayores restricciones respecto de los datos que comparte con anunciantes a través de su plataforma de subasta de anuncios, como consecuencia de la investigación que comenzó la autoridad irlandesa de protección de datos sobre el tratamiento de datos personales en el contexto

97. *Ver* Alexander Dhoest y Lukasz Szulc, *Navigating online selves: social, cultural, and material contexts of social media use by diasporic gay men*, Social Media + Society, 2016, http://eprints.lse.ac.uk/87145/1/Szulc_Navigating%20online%20selves_2018.pdf

98. Kashmir Hill, *How Facebook Outs Sex Workers*, Gizmodo, noviembre de 2017, https://gizmodo.com/how-facebook-outs-sex-workers-1818861596

99. Julie E. Cohen, 2013

100. Sundar Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, New York Times, 7 de mayo de 2019

101. Facebook, *A Privacy-Focused Vision for Social Networking*, 6 de marzo de 2019, https://newsroom.fb.com/news/2019/03/vision-for-social-networking/

102. Kurt Wagner y Selina Wang, *Facebook's Zuckerberg Preaches Privacy, But Evidence Is Elusive*, Bloomberg, 1 de mayo de 2019

103. Además, ambas empresas hicieron referencia a las herramientas que ofrecen a los usuarios para que puedan controlar sus preferencias respecto de los anuncios. Ver Google, *Control the ads you see*, https://support.google.com/accounts/answer/2662856; Facebook https://facebook.com/help/247395082112892

de Ad Exchange de Google.[104] Google lanzó una nueva función que les permite a los usuarios borrar los datos de ubicación (aunque solamente después de que hayan estado guardados por un período mínimo de tres meses).[105] Por su parte, Facebook comenzó a implementar una herramienta que permite a los usuarios ver la información que otras aplicaciones y sitios web comparten con Facebook y desvincular los datos de sus cuentas (aunque no permite eliminarlos por completo).[106]

Si bien esto podría ser un presagio positivo de que vendrán mejores prácticas de privacidad, muchos analistas se han mostrado escépticos ante la idea de que Google y Facebook cambien sustancialmente, precisamente porque su modelo de negocios y su posición como dos de las empresas más grandes que cotizan en bolsa se basan en la vigilancia.[107] En julio de 2019, la Comisión Federal de Comercio de los Estados Unidos llegó a un acuerdo con Facebook respecto de las violaciones a la privacidad en virtud del cual la empresa está obligada a reestructurar sus prácticas de privacidad y a someterse a nuevos requisitos de privacidad y a un control.[108] Sin embargo, como se explica en detalle en el capítulo 4, estos cambios no abordan a fondo la cuestión del modelo de negocios de la empresa ni su impacto inherente respecto de la privacidad.

Ambas empresas tienen un largo historial de escándalos y promesas no cumplidas en torno a la privacidad, lo que pone de relieve las consecuencias del modelo de negocios basado en la vigilancia sobre la privacidad y genera interrogantes sobre las promesas de estas marcas de cambiar dicho modelo.

Tanto Google como Facebook han recibido críticas públicas por sus prácticas de privacidad que datan de más de una década. En 2007, el primer esfuerzo de Facebook de instalar anuncios invasivos en su plataforma, conocido como el proyecto Beacon, fue tan mal recibido que la empresa tuvo que suspenderlo.[109] Por otro lado, durante muchos años hubo protestas públicas contra los anuncios segmentados de Gmail, y en 2017 la empresa anunció que ya no analizaría los mensajes de correo electrónico para generar publicidad personalizada.[110] Una vez que hay suficientes personas conscientes de la vigilancia que se quejan al respecto, las empresas suelen optar por disculparse, pero, mientras tanto, este modelo de negocios ha tendido inexorablemente hacia la vigilancia en su máxima expresión, como se describió en párrafos anteriores.

Además, se sabe que Google y Facebook ya han incurrido en prácticas engañosas para los usuarios en materia de privacidad y publicidad segmentada. Veamos algunos ejemplos:

- Durante el desarrollo de Google Street View en 2010, los automóviles de Google que fotografiaban las calles también recopilaban, en secreto, mensajes privados de correo electrónico y contraseñas de redes inalámbricas no seguras.[111]
- En 2018, los periodistas descubrieron que Google mantiene activada la función que rastrea la ubicación de los usuarios incluso cuando ha sido desactivada. Luego de que la noticia saliera a la luz, Google modificó la descripción de la función, pero esta sigue rastreando la ubicación aun cuando los usuarios desactivan el historial de ubicaciones.[112] Actualmente, Google enfrenta

104. Google, *Additional steps to safeguard user privacy,* 14 de noviembre de 2019, https://www.blog.google/products/admanager/additional-steps-safeguard-user-privacy; Irish Data Protection Commission, *Data Protection Commission opens statutory inquiry into Google Ireland Limited,* 22 de mayo de 2019

105. Google, *Introducing auto-delete controls for your Location History and activity data*, 1 de mayo de 2019, https://www.blog.google/technology/safety-security/automatically-delete-data . Google también hizo referencia a su trabajo orientado a desarrollar tecnologías de aprendizaje federado, ver https://federated.withgoogle.com/.

106. Facebook, *Now You Can See and Control the Data That Apps and Websites Share With Facebook*, 20 de agosto de 2019, https://about.fb.com/news/2019/08/off-facebook-activity/

107. En palabras de Shoshana Zuboff: "¿cómo podemos esperar que las empresas cuya existencia económica depende del excedente conductual dejen de recopilar datos sobre nuestros comportamientos por voluntad propia? Sería como pedirles que se suiciden". Zuboff, *The Secrets of Surveillance Capitalism*, Frankfurter Allgemeine, marzo de 2016; Ver también, p. ej., Bruce Schneier, *A New Privacy Constitution for Facebook*, 8 de marzo de 2019; Casey Johnston, *Facebook is trying to make the word "private" meaningless*, The Outline, 1 de mayo de 2019; Julia Carrie Wong, *My data security is better than yours: tech CEOs throw shade in privacy wars*, 9 de mayo de 2019

108. Facebook, *A New Framework for Protecting Privacy*, 24 de julio de 2019, https://about.fb.com/news/2019/07/ftc-agreement/

109. The Register, *Facebook turns out light on Beacon*, 23 de septiembre de 2009

110. Google, *As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align*, 23 de junio de 2017

111. Guardian (RU), *Google admits collecting Wi-Fi data through Street View cars*, 15 de mayo de 2010, https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data

acciones legales por este tema a raíz de la demanda del órgano que controla la competencia en Australia.[113]

- Según una investigación periodística de principios de 2019, los dispositivos para el hogar de Google Nest contenían un micrófono sobre el que no se había informado al público.[114]
- Facebook reconoció que sabía de las violaciones de los datos en las que incurría la agencia de microsegmentación política Cambridge Analytica meses antes de que estallara el escándalo (ver recuadro en la capítulo 3 más adelante).[115]
- A través de una aplicación llamada Facebook Research, Facebook les pagaba a los adolescentes para que descargaran una aplicación que rastreaba cada acción que realizaban en su teléfono.[116]
- Facebook también admitió haber realizado experimentos conductuales sobre grupos de personas; por ejemplo, influyó en ciertos ciudadanos para que votaran y les levantó (o bajó) el ánimo a algunos usuarios mostrándoles diversos contenidos en la sección de noticias.[117]

Resulta difícil no concluir que las numerosas violaciones de la privacidad en las que incurrieron ambas empresas no son irregularidades sino que, en cambio, demuestran exactamente cómo el modelo basado en la vigilancia de Google y Facebook se sustenta sobre la capacidad de ambos gigantes de recopilar, analizar y vender grandes volúmenes de datos sin considerar el derecho a la privacidad.

EL ACCESO DE LOS ESTADOS A LAS BÓVEDAS DE DATOS DE GOOGLE Y FACEBOOK

"Hay que suponer que cualquier dato personal almacenado por Facebook o Android es información que los gobiernos de todo el mundo intentarán obtener o que los ladrones tratarán de robar".

Tim Wu, 2019[118]

Además del impacto directo que ya tiene sobre la privacidad el modelo de negocios basado en la vigilancia, también existe el riesgo de las consecuencias indirectas producto de la relación entre la vigilancia corporativa y los programas de vigilancia estatales. Las autoridades estatales, como las agencias de inteligencia, de aplicación de la ley y de inmigración, buscan cada vez más obtener acceso a los datos que están en manos de las empresas de tecnología.[119] Las inmensas bóvedas de datos que poseen Google y Facebook son como un gran "tarro de miel" centralizado para las autoridades estatales, que las ven como una oportunidad para acceder a datos personales sumamente valiosos que, de lo contrario, sería muy difícil de reunir.

Como tal, el modelo conlleva el riesgo inherente de que Google y Facebook puedan contribuir a que los Estados incurran en una vigilancia digital invasiva e ilegal o violen de alguna forma los derechos

112. Associated Press, *Google clarifies location-tracking policy*, agosto de 2018, https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211

113. Comisión Australiana de Competencia y Consumo (ACCC), *Google allegedly misled consumers on collection and use of location data*, 29 de octubre de 2019, https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data

114. The Verge, *Google claims built-in Nest mic was 'never intended to be a secret'*, febrero de 2019 https://www.theverge.com/circuitbreaker/2019/2/20/18232960/google-nest-secure-microphone-google-assistant-built-in-security-privacy

115. Guardian (RU), *Facebook acknowledges concerns over Cambridge Analytica emerged earlier than reported*, 22 de marzo de 2019, https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing

116. Josh Constine, *Facebook admits 18% of Research spyware users were teens, not <5%,* TechCrunch, 28 de febrero de 2019, https://techcrunch.com/2019/02/28/facebook-research-teens/

117. Christian Science Monitor, *Facebook 'I Voted' button experiment: praiseworthy or propaganda?*, noviembre de 2014; Guardian (RU), *Facebook reveals news feed experiment to control emotions*, junio de 2014

118. Tim Wu, autor de 'The Attention Merchants', *How Capitalism Betrayed Privacy*, New York Times, 10 de abril de 2019, https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html

119. Ver, por ejemplo, CNBC, *US, UK sign first-ever deal to access data from tech companies like Facebook and Google*, octubre de 2019, https://www.cnbc.com/2019/10/04/us-uk-sign-agreement-to-access-data-from-tech-companies-like-facebook.html ; Jennifer Lynch, EFF, *Google's Sensorvault Can Tell Police Where You've Been*, abril de 2018, https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been

de las personas. Aunque este riesgo existe en el caso de todas las empresas que acumulan enormes bóvedas de datos personales, el modelo de negocios basado en la vigilancia que utilizan Google y Facebook fomenta que estas empresas recopilen y posean tantos datos como sea posible para así aumentar sus ingresos, lo que hace que el riesgo sea mayor.

Las revelaciones de vigilancia masiva expuestas por Edward Snowden, el antiguo informante de la Agencia Nacional de Seguridad (NSA) de Estados Unidos, dejaron en evidencia las formas en que las agencias de inteligencia habían podido acceder a los datos de las empresas de tecnología. Los documentos de inteligencia estadounidense que divulgó Snowden en 2013 dejaron al descubierto que las agencias de inteligencia de los Estados Unidos y el Reino Unido llevaban a cabo programas de vigilancia indiscriminada a gran escala, y que empresas como Yahoo, Google y Microsoft habían tenido que responder a ordenamientos jurídicos secretos y entregar datos de sus clientes.[120] La NSA también pudo eludir las protecciones de seguridad de Google y Yahoo para acceder a los centros de datos de ambas empresas.[121]

A raíz de las divulgaciones de Snowden, las empresas de tecnología han extendido el uso del cifrado para proteger los datos de sus usuarios y han presentado recursos judiciales contra los pedidos de los Estados para acceder a los datos de los usuarios, como ocurrió en el caso del gobierno estadounidense, que recurrió a órdenes judiciales que prohibían a las empresas divulgar ciertos tipos de pedidos de información que reciben por vía legal.[122] Tanto Google como Facebook son miembros de la coalición Reform Government Surveillance (RGS), que promueve una reforma de la legislación y las prácticas que regulan la vigilancia gubernamental.[123] Si bien estas medidas son bienvenidas, lo cierto es que no abordan la causa subyacente del problema, que es que el modelo de negocios basado en la vigilancia incentiva la recopilación y el procesamiento de datos a gran escala de tal manera que amplía enormemente las oportunidades de vigilancia estatal.

DERECHOS HUMANOS EN GOOGLE Y FACEBOOK

En consonancia con las normas internacionales de derechos humanos, Google y Facebook deberían llevar a cabo el proceso de diligencia debida y abordar las consecuencias potenciales y actuales de su modelo de negocio con respecto a derechos humanos específicos, como los derechos a la privacidad y la libertad de expresión.[124] Ahora bien, la recolección, el análisis y la monetización de los datos son parte fundamental de su modelo de negocios. Al mismo tiempo, esto tiene efectos fundamentales y generalizados sobre el derecho a la privacidad y, por lo demás, es inherentemente contrario al ejercicio de ese derecho. Por consiguiente, ambas empresas también deberían evaluar si el modelo de negocio basado en la vigilancia podría alguna vez ser compatible con su responsabilidad de respetar los derechos humanos.

Tanto Google como Facebook han asumido un compromiso de larga data con los derechos a la privacidad y la libertad de expresión, al participar en la Iniciativa de Red Global (GNI).[125] Sin embargo, la Iniciativa de Red Global solo aborda los riesgos para la libertad de expresión y la privacidad, no para

120. Ewen MacAskill y Dominic Rushe, *Snowden document reveals key role of companies in NSA data collection*, Guardian (RU), noviembre de 2013 https://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms

121. Bartom Gellman y Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, The Washington Post, octubre de 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

122. Washington Post, *Google challenges U.S. gag order, citing First Amendment,* 18 de junio de 2013

123. Reform Government Surveillance, *RGS Principles*, https://www.reformgovernmentsurveillance.com/principles/

124. Ranking Digital Rights lleva a cabo una evaluación detallada de las principales empresas de Internet, de telefonía móvil y de telecomunicaciones respecto de sus políticas y compromisos públicos en relación con la libertad de expresión y la privacidad de los usuarios de Internet en todo el mundo. *Ver 2019 Ranking Digital Rights Corporate Accountability Index,* https://rankingdigitalrights.org/index2019. Actualmente, RDR está ampliando su metodología para abordar el daño relacionado con la implementación de prácticas y políticas de anuncios dirigidos por parte de las empresas y el uso y desarrollo de sistemas de toma de decisiones basados en algoritmos.

125. Ver también los principios de inteligencia artificial (IA) de Google https://ai.google/principles, así como la declaración sobre derechos humanos de Google https://about.google/human-rights/

otros derechos. Además, se enfoca principalmente en la respuesta de las empresas ante los pedidos de datos por parte de los Estados.

A través de la GNI, ambas empresas están sujetas a evaluaciones independientes cada dos años, en las que se revisan sus sistemas, políticas y procedimientos internos relevantes. La evaluación más reciente publicada en julio de 2016 concluyó que las dos empresas cumplían con los Principios de la GNI, los cuales se basan en las leyes y normas de derechos humanos reconocidas en todo el mundo.[126]

Dado que el proceso es confidencial, Amnistía Internacional no puede verificar esta evaluación. No obstante, GNI afirma que el alcance de su proceso evaluativo comprende un examen de los sistemas, las políticas y los procedimientos empresariales, junto con una evaluación de un número de casos específicos acordados con cada empresa.[127] Ahora bien, el foco en casos prácticos puntuales podría indicar que el proceso no implica una evaluación holística respecto de si la empresa realmente implementa estas políticas y procedimientos en la práctica, lo que incluiría identificar y abordar el impacto en los derechos humanos en todos los aspectos de su negocio. Este enfoque también podría sugerir que la evaluación no analiza si empresas como Google y Facebook están realizando la diligencia debida necesaria para identificar y atender las consecuencias que tiene su modelo de negocios en general para los derechos humanos. Por lo tanto, dicho proceso parece no abordar el problema de fondo que se analiza en este informe, esto es, si el modelo de negocios basado en la vigilancia puede llegar a ser compatible con la responsabilidad que tienen las empresas de respetar los derechos humanos, siendo que, de base, este modelo es contrario a los tres elementos fundamentales del derecho a la privacidad.[127]

Amnistía Internacional les preguntó a Google y Facebook si sus procesos de diligencia debida sobre derechos humanos contemplaban los efectos sistémicos y generalizados sobre los derechos de su modelo de negocios en general, en especial, con respecto al derecho a la privacidad, como se describió anteriormente. En el marco de una reunión con Amnistía Internacional, Google sostuvo que lleva a cabo procesos de diligencia debida en materia de derechos humanos en toda su empresa. Facebook envió una carta con una respuesta detallada (ver anexo), pero no respondió esta pregunta en particular.

126. GNI, *2015/2016 Company Assessments*, julio de 2016, https://globalnetworkinitiative.org/2015-2016-company-assessments/

127. GNI, *Company Assessments*, https://globalnetworkinitiative.org/company-assessments/

128. El proceso de revisión del ciclo de evaluación actual de la GNI incluye preguntas como en qué consiste la diligencia debida que realiza la empresa a fin de identificar potenciales riesgos para la libertad de expresión y la privacidad en relación con determinados productos, mercados, adquisiciones o relaciones comerciales, pero no aborda el modelo de negocios de la empresa en su conjunto. Ver: GNI, *2018/2019 Company Assessments*, Appendix I: Process Review Questions, https://globalnetworkinitiative.org/wp-content/uploads/2019/03/GNI-2018-Appendix-I.pdf

3. ANALÍTICA DE DATOS A GRAN ESCALA: RIESGOS PARA LOS DERECHOS HUMANOS MÁS ALLÁ DE LA PRIVACIDAD

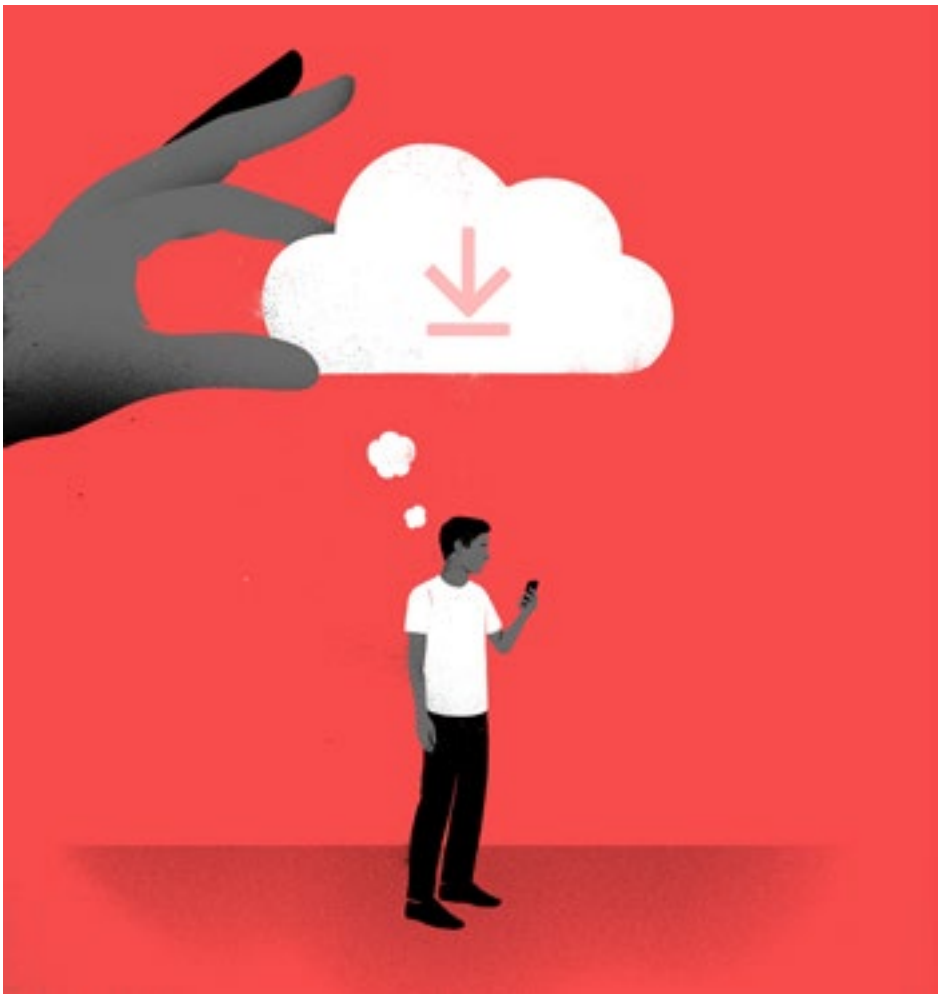
> ***"La vigilancia consiste meramente en observar, ¿pero cómo ha afectado a la sociedad? ¿Cuáles son las consecuencias cuando no hay espacios donde acceder a puntos de vista disidentes o para experimentar con la autopresentación de distintas formas? ¿Qué implica esto? En realidad, es una forma de control social... un avance hacia el conformismo... La palabra vigilancia en sí no es lo suficientemente agresiva como para describir este fenómeno".***
>
> —Julia Angwin, 2018[129]

Las plataformas de Google y Facebook están respaldadas por un conjunto de sistemas de analítica de datos de avanzada. Sus modelos algorítmicos están diseñados para presentar contenido "relevante" al usuario (relevante según lo que infieren las empresas en función de los datos recopilados), lo que incluye tanto publicaciones orgánicas como anuncios. Por ejemplo, los algoritmos de Google Search y la sección de noticias de Facebook se nutren constantemente de grandes cantidades de datos de

129. Julia Angwin, en diálogo con Trevlor Paglen, *The End of Trust*, número 54, McSweeney's Quarterly Concern y Electronic Frontier Foundation, p. 55, https://www.eff.org/document/end-trust-0.

los usuarios para cumplir diversos propósitos, como mostrarles anuncios, brindarles resultados de búsqueda, recomendarles contenido e incentivar a los usuarios a que generen contenido nuevo e interactúen con el que ya existe. Para ello, los sistemas desempeñan tareas de "optimización", a fin de entregar de la mejor forma posible los resultados más específicos, con base en procesos algorítmicos iterativos y altamente complejos que generan correlaciones e inferencias a partir de los datos de los usuarios.[130]

Cada vez más, vemos que estos sistemas algorítmicos generan efectos en cadena que pueden derivar en graves repercusiones negativas para los derechos humanos, entre ellos, la privacidad, la libertad de expresión y el derecho a la igualdad y a la no discriminación.[131] En algunos casos, esas repercusiones son provocadas directamente por la tecnología que utiliza la empresa; en otros, son producto de la explotación de dichas herramientas por parte de terceros que las usan en perjuicio de los derechos humanos. Además, esas repercusiones se amplifican y multiplican considerablemente a causa de la enorme magnitud de las operaciones de Facebook y Google, así como del predominio de estas plataformas.



130. "Los sistemas de optimización aplican una lógica de control operativo orientada a los resultados más que al proceso... Cuando hablamos de sistemas de optimización, nos referimos a aquellos sistemas que captan y manipulan el comportamiento del usuario y sus entornos de acuerdo con la lógica de la optimización". Rebekah Overdorf, Bogdan Kulynych, Ero Balsa, Carmela Troncoso, Seda Gürses, *POTs: Protective Optimization Technologies,* agosto de 2018, https://arxiv.org/abs/1806.02711.

131. Ver varios ejemplos citados en Ranking Digital Rights, *Human Rights Risk Scenarios:* Targeted Advertising, febrero de 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf; y Algorithms, machine learning and automated decision-making, julio de 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf

Como resultado, el daño inicial causado por el ataque a la privacidad producto del modelo basado en la vigilancia tiene un efecto búmeran sobre las personas e impacta en ellas en miles de formas inesperadas. Por ejemplo, a nivel individual, la persona podría ceder algunos datos aparentemente inofensivos, como el contenido que le gusta en Facebook. Al consolidarse, esos datos pueden usarse con un propósito diferente, como mostrar anuncios, mensajes políticos y propaganda finamente segmentados, o para llamar la atención de los usuarios y hacer que permanezcan en la plataforma.

El ACNUDH ha afirmado que la potencia analítica de la tecnología basada en datos ha dado origen a un entorno que "entraña riesgos para las personas y las sociedades que no deben subestimarse".[132]

MAYOR PERSONALIZACIÓN, ELABORACIÓN DE PERFILES Y MICROSEGMENTACIÓN

La analítica de datos avanzada es una parte central del modelo de negocios basado en la vigilancia y ha catapultado el poder económico de Facebook y Google. En 2018, Facebook anunció que uno de los marcos de aprendizaje automático en los que se basa su plataforma arrojaba 200 billones de predicciones por día.[133] Los sistemas algorítmicos estimulan el modelo de negocios de dos formas clave: primero, al mostrar anuncios segmentados; segundo, al maximizar las interacciones de los usuarios. Como se indica en las secciones subsiguientes, ambos propósitos tienen efectos secundarios alarmantes que atentan contra los derechos humanos.[134]

La acumulación de datos les permite a Facebook y Google mostrar anuncios altamente segmentados a los usuarios, de acuerdo con una compleja combinación de las características de su perfil, como su ubicación, datos demográficos, intereses y comportamiento. Como se describió en el capítulo 1, los encargados de inferir y predecir estas características son los sofisticados modelos algorítmicos de las empresas. La capacidad de Google y Facebook de ofrecerles a los anunciantes minuciosas herramientas de predicción y microsegmentación ha incrementado considerablemente los ingresos por publicidad para estas empresas.

La publicidad segmentada es un ecosistema complejo conformado por una gran cantidad de empresas y otras entidades. No obstante, la combinación singular de sus bases de datos de manera que se refuerzan mutuamente, el alcance de sus plataformas y el control respecto de los principales flujos de datos, así como la consecuente capacidad de ambas empresas para desarrollar las herramientas de aprendizaje automático y los modelos de predicción más avanzados, implican que Google y Facebook dominan por completo el mercado de la publicidad digital.

Además de implementar analítica de datos con fines publicitarios, Facebook y Google también utilizan algoritmos para personalizar la experiencia del usuario y "maximizar las interacciones" con sus productos, de modo que las personas permanezcan en sus plataformas el mayor tiempo posible.[135] En definitiva, estos sitios están diseñados para ser adictivos.[136] Este mecanismo está íntimamente relacionado con el modelo de negocios y con los ingresos de ambas empresas, ya que cuanto más tiempo pasan los usuarios en cada plataforma, más anuncios presenta el sistema, y más personas los ven y hacen clic en ellos, lo que a su vez genera más datos. Asimismo, este proceso refuerza el modelo al asegurar el acceso continuo a los datos de las personas y preservar la hegemonía de las plataformas.

---

132. ACNUDH, *El derecho a la privacidad en la era digital*, 3 de agosto de 2018, A/HRC/39/29, párrafo 16.

133. Facebook, *Announcing PyTorch 1.0 for both research and production*, mayo de 2018, https://engineering.fb.com/ai-research/announcing-pytorch-1-0-for-both-research-and-production

134. Ranking Digital Rights, *Human Rights Risk Scenarios:* Targeted Advertising, febrero de 2019; and Algorithms, machine learning and automated decision-making, julio de 2019

135. Facebook niega que su algoritmo de la sección de noticias esté diseñado para maximizar la participación de los usuarios y sostiene que "el objetivo es conectar a los usuarios con contenido que sea interesante y relevante para ellos". Ver la respuesta de Facebook en el anexo que se incluye.

136. ABC News, *extracto del libro: 'Ten Arguments for Deleting Your Social Media Accounts Right Now',* de Jaron Lanier, junio de 2018, https://abcnews.go.com/Technology/book-excerpt-jaron-laniers-ten-arguments-deleting-social/story?id=56009512.

INFLUIR EN LA OPINIÓN Y LAS CREENCIAS DE LAS PERSONAS

Como se describió en el capítulo 2, la privacidad está íntimamente vinculada con el concepto de autonomía, es decir, la capacidad de moldear y expresar nuestra identidad sin la observación injustificada y la influencia indebida de terceros.

No obstante, la combinación de la segmentación de anuncios y el contenido personalizado según los algoritmos significa que las plataformas de Google y Facebook tienen un rol preponderante en la configuración de la experiencia en línea de las personas y en la determinación de la información que vemos. Esto puede influenciar, moldear y modificar nuestros pensamientos y opiniones, lo que puede afectar nuestra capacidad para tomar decisiones de manera autónoma. Más aún, los algoritmos están diseñados para encontrar las mejores formas de orientar a las personas hacia determinados resultados en función de las características personales únicas de cada sujeto. Al respecto, la tecnosocióloga Zeynep Tufekci ha descrito las plataformas como "arquitecturas de persuasión", capaces de manipular e influenciar a miles de millones de personas.[137] En consonancia con ello, James Williams, ex encargado de estrategia publicitaria de Google, se ha referido a este fenómeno como la "industrialización de la persuasión", aludiendo a que la "conquista y explotación de nuestra atención" nos distrae a tal punto que limita nuestra capacidad para pensar con claridad y trabajar para alcanzar nuestras metas.

Semejantes capacidades implican un alto riesgo de que estas empresas puedan perjudicar directamente los derechos de las personas a la libertad de pensamiento, conciencia y religión, y la libertad de opinión y expresión, a través del uso de sus sistemas algorítmicos.[138] Al mismo tiempo, corren el riesgo de contribuir a las violaciones de estos derechos perpetradas por otras personas y entidades que tienen la capacidad para acceder a sus modelos o utilizarlos.

Las normas internacionales relativas a los derechos humanos no permiten ningún tipo de limitación a la libertad de pensamiento y conciencia o la libertad para tener o adoptar una religión o creencia a elección de cada persona. Dichas libertades están protegidas incondicionalmente, al igual que el derecho de toda persona de tener sus propias opiniones sin ser objeto de injerencia alguna.[139] El Comité de Derechos Humanos ha concluido que el derecho a la libertad de opinión requiere que las personas no estén sujetas a ninguna forma de coerción indebida en el desarrollo de sus creencias, ideologías, reacciones y posturas.[140] El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas ha destacado que "la intersección entre tecnología y curación de contenido genera nuevos interrogantes acerca de los tipos de coerción o inducción que podrían considerarse como una injerencia en el derecho a formar una opinión"[141]. También ha observado que "las empresas deben, por lo menos, proporcionar información significativa sobre cómo desarrollan e implementan criterios para curar y personalizar el contenido en sus plataformas, incluyendo las políticas y los procesos que utilizan para detectar sesgos sociales, culturales o políticos al diseñar y desarrollar sistemas de inteligencia artificial relevantes".[142] Por su parte, el Comité de Ministros del Consejo de Europa también ha advertido que "los niveles de persuasión detallada, subconsciente y personalizada podrían tener efectos significativos sobre la

137. Zeynep Tufekci, *We're building a dystopia just to make people click on ads*, TEDGlobal, septiembre de 2017, https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads/transcript?language=en

138. Derechos garantizados por los artículos 18, 19 de la Declaración Universal de los Derechos Humanos; artículos 18, 19 del Pacto Internacional de Derechos Civiles y Políticos.

139. Ver Comité de Derechos Humanos, "Observación general n. 22: El derecho a la libertad de pensamiento, de conciencia y de religión (art. 18), 30 de julio de 1993, CCPR/C/21/Rev/1/Add/4, párrafo 3, y Comité de Derechos Humanos, "Observación general n. 34, art. 19: Libertad de opinión y libertad de expresión", CCPR/C/GC/43, 12 de septiembre de 2011, párrafo 3.

140. *Yong Joo-Kang c. República de Corea,* Comité de Derechos Humanos, comunicación n.º 878/1999, 16 de julio de 2003 (CCPR/C/78/D/878/1999).

141. David Kaye, Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, informe presentado en la Asamblea General de la ONU, 29 de agosto de 2018, A/73/348, párrafo 24. (David Kaye, 2018)

142. David Kaye, 2018, párrafo 26 Como se sostuvo anteriormente, Facebook ha dado algunos pasos en esta dirección, por ejemplo, con las herramientas que les brindan a los usuarios "más información y control sobre lo que ven en Facebook". Ver la respuesta de Facebook en el anexo que se incluye.

autonomía cognitiva de las personas y su derecho a formar una opinión propia y tomar decisiones de manera independiente".[143]

Hay varios ejemplos que demuestran cómo pueden utilizarse las plataformas para dirigir contenidos específico a las personas y así influir en su opinión y sus creencias. La segmentación con este grado de detalle es posible a causa del modelo de negocios basado en la vigilancia de Facebook y Google. Según ciertas investigaciones académicas, ahora el aprendizaje automático es capaz de escanear las fotos de Instagram y detectar signos de depresión de forma mucho más confiable que los revisores humanos[144]. Facebook también les dijo a los anunciantes que sus sistemas podían juzgar cuándo los adolescentes se sentían "inseguros" o "inútiles", o cuándo necesitaban un "refuerzo de autoestima"[145]. En respuesta, Facebook afirmó que no permite segmentar audiencias por estado emocional;[146] de todas formas, el caso resalta las capacidades de la plataforma y el modo en que esta podría utilizarse abusivamente para dirigirse a las personas de manera intrusiva en sus momentos de mayor vulnerabilidad.

Otro ejemplo es el método de redireccionamiento de Google, un proyecto que utiliza la plataforma de AdWords de la empresa (actualmente conocida como Google Ads) para desradicalizar a potenciales defensores del terrorismo islámico.[147] Un especialista utilizó esa misma herramienta, que se encuentra disponible libremente en Internet, para incentivar a personas suicidas a llamar a una línea de ayuda.[148] Estos casos demuestran que la "ingeniería social" podría ser utilizada sin mayores dificultades para manipular las opiniones y creencias de las personas, ya sea por las empresas de forma directa o por otras personas o entidades. Si bien en los últimos ejemplos dicha influencia se usó con un objetivo presuntamente positivo, sería muy sencillo utilizar estas mismas herramientas para perjudicar nuestros derechos, en especial si se implementan a gran escala.

MANIPULACIÓN OCULTA A GRAN ESCALA

El derecho a la privacidad es "un requisito esencial para el ejercicio del derecho a la libertad de expresión"[149] y, por lo tanto, la erosión de la "esfera privada" que propician Google y Facebook tiene sus correspondientes efectos directos e indirectos en el libre desarrollo e intercambio de ideas.

La libertad de expresión es un derecho colectivo que habilita a las personas a buscar y recibir información como grupo social y a "expresar sus opiniones colectivas".[150] Por su propia naturaleza, los sistemas algorítmicos repercuten en las personas como un grupo, además de hacerlo en cada sujeto a nivel individual.[151] Cuando las capacidades de influencia y persuasión se implementan a gran escala, como lo hacen las plataformas controladas por Facebook y Google, las empresas tienen la capacidad de influir en la opinión de grandes grupos o segmentos de la población, lo que a su vez puede dar lugar a la explotación por parte de otras personas o entidades.

---

143. Comité de Ministros del Consejo de Europa, *Declaration on the Manipulative Capabilities of Algorithmic Processes*, febrero de 2019, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

144. Johannes C. Eichstaedt, Robert J. Smith, Raina M. Merchant, Lyle H. Ungar, Patrick Crutchley, Daniel Preoţiuc-Pietro, David A. Asch y H. Andrew Schwartz, *Facebook language predicts depression in medical records*, octubre de 2018, https://www.pnas.org/content/115/44/11203.

145. The Australian, *Facebook targets 'insecure' kids*, mayo de 2017, https://www.theaustralian.com.au/business/media/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

146. Facebook, *Comments on Research and Ad Targeting*, abril de 2017, https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting/

147. The Redirect Method, https://redirectmethod.org/

148. Patrick Berlinquette, *I Used Google Ads for Social Engineering. It Worked.* New York Times, julio de 2019 https://www.nytimes.com/2019/07/07/opinion/google-ads.html

149. Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, 17 de abril de 2013, A/HRC/23/40, párrafo 24.

150. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, 20 de abril de 2010, A/HRC/14/23, párrafo 29.

151. "Un perfil no identifica simplemente las características de titulares de datos individuales; antes bien, estas se construyen por contraste con otros titulares en el conjunto de datos". Lilian Edwards y Michael Veale, *Slave to the Algorithm? Why A 'Right To An Explanation' Is Probably Not The Remedy You Are Looking For,* 16 Duke Law & Technology Review 18, 2017, p. 35, https://ssrn.com/abstract=2972855 (Edwards y Veale, 2017)

El modelo de negocios basado en la vigilancia ha creado una arquitectura que no solamente ha reducido y restringido la "esfera privada", sino que, al mismo tiempo, ha aislado a las personas entre sí, ya que cada sujeto interactúa con su propia experiencia personalizada de Internet, la cual está diseñada específicamente a la medida de cada persona, en función de varias inferencias y la elaboración de perfiles basados en algoritmos.[152] Este fenómeno deja la puerta abierta a la violación de los derechos de las personas mediante la manipulación masiva.

El ejemplo más claro y visible de cómo las capacidades de segmentación detallada de Facebook y Google pueden utilizarse de manera indebida contra las personas está en el ámbito de las campañas políticas, siendo el escándalo en torno a Cambridge Analytica el caso de mayor repercusión mediática (ver recuadro). Los mismos mecanismos y herramientas de persuasión que se utilizan con fines publicitarios pueden usarse también para influenciar y manipular las opiniones políticas de las personas.[153] Además, el uso de la microsegmentación aplicada a menajes políticos puede limitar la libertad de expresión de las personas al "crear una visión curada del mundo en la que no hay lugar para el pluralismo en el discurso político".[154]

EL ESCÁNDALO DE CAMBRIDGE ANALYTICA

Cambridge Analytica era una empresa de analítica de datos políticos que afirmaba tener la habilidad para influenciar a poblaciones a través de la creación de perfiles de personalidad para mostrarles a las personas mensajes políticos acordes con su perfil, técnica que se conoce como segmentación psicográfica.[155] Desde el propio marketing de Cambridge Analytica se sostenía que la empresa tenía perfiles de hasta 240 millones de estadounidenses y que tenía entre 4000 y 5000 puntos de datos respecto de cada votante.[156]

En 2014, Cambridge Analytica obtuvo acceso a datos de perfiles de Facebook a través de una aplicación con el nombre de "thisisyourdigitallife", creada por el Dr. Aleksander Kogan, profesor de psicología de Cambridge University. Cuando los usuarios de Facebook descargaban la aplicación, la autorizaban a acceder a su información personal.[157] La empresa del Dr. Kogan celebró un contrato con una sociedad vinculada con Cambridge Analytica con el objeto de recopilar datos de Facebook.[158]

De acuerdo con las políticas de Facebook de aquel entonces, las aplicaciones podían acceder no solo a los datos de los usuarios que otorgaban su consentimiento de forma directa, sino también a los de las personas que formaban parte de la red social de esos usuarios (p. ej., sus amigos de Facebook).[159] Como consecuencia de esto, si bien solo 270.000 usuarios prestaron su consentimiento para compartir sus datos a través de la aplicación de Kogan, se terminó compartiendo indebidamente información de hasta 87 millones de perfiles de Facebook con Cambridge Analytica, según una confirmación posterior por parte de Facebook.[160]

152. Por ejemplo, según un estudio realizado por la Web Foundation sobre la curación del contenido que se muestra en la sección de noticias de Facebook, "el algoritmo coloca a cada usuario en una versión aparte y personalizada de lo que debería ser una plaza pública con información". Ver Web Foundation, *The Invisible Curation of Content*, 2018, p. 5: http://webfoundation.org/docs/2018/04/WF_InvisibleCurationContent_Screen_AW.pdf

153. Tactical Tech ha investigado y detallado las herramientas y técnicas empleadas en la industria de los datos políticos. Ver Tactical Tech, *Tools of the Influence Industry*, https://ourdataourselves.tacticaltech.org/posts/influence-industry

154. David Kaye, 2018, párrafo 18

155. Sue Halpern, *Cambridge Analytica and the Perils of Psychographics*, The New Yorker, https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics

156. BBC News, *Cambridge Analytica parent firm SCL Elections fined over data refusal,* enero de 2019

157. Facebook, *Suspending Cambridge Analytica and SCL Group From Facebook*, marzo de 2018 https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/

158. Carole Cadwalladr y Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, Guardian (RU), 17 de marzo de 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

159. Comité de Tecnología Digital, Cultura, Medios y Deportes de la Cámara de los Comunes del Reino Unido, *Interim Report into Disinformation and 'fake news'*, julio de 2018, párrafo 120

160. Facebook, *An Update on Our Plans to Restrict Data Access on Facebook*, 4 de abril de 2018, https://newsroom.fb.com/news/2018/04/restricting-data-access/

A fines de 2015, The Guardian informó que Cambridge Analytica estaba usando indebidamente datos personales extraídos de Facebook para la campaña del candidato a presidente de los Estados Unidos Ted Cruz.[161] Como respuesta, Facebook pidió a Kogan y Cambridge Analytica que borraran los datos.[162] Si bien Cambridge Analytica aseveró que eliminaría los datos, siguió teniendo acceso a ellos o a modelos basados en esos datos.[163]

En 2016, los asesores de la campaña de Donald Trump para presidente de los EE. UU. contrataron al equipo de Cambridge Analytica, que utilizó los perfiles psicográficos con el fin de ayudarlos a identificar audiencias objetivo para mostrarles anuncios digitales e influenciar la concurrencia del electorado. No fue sino hasta abril de 2018, después de que The Observer y el New York Times difundieran la historia de cómo Cambridge Analytica había usado datos de Facebook, que Facebook comenzó a contactar a los 87 millones de usuarios afectados por la violación de datos.[163]

Hay tres aspectos fundamentales del escándalo en torno a Facebook. En primer lugar, las políticas de privacidad de datos que Facebook implementaba en ese momento, y que eran claramente muy laxas, le permitieron al Dr. Kogan obtener información personal, no solo de los usuarios de Facebook que habían accedido a la aplicación, sino también de todos los miembros de sus redes sociales. Posteriormente, Facebook tuvo que suspender decenas de miles de aplicaciones de alrededor de 400 desarrolladores que habían tenido acceso a los datos de los usuarios antes de que, en 2014, la empresa restringiera ese acceso para los desarrolladores.[165] Desde ese momento, Facebook ha restringido en gran medida el alcance del acceso a los datos de los usuarios que tienen los desarrolladores de aplicaciones.[166] En segundo lugar, aunque Facebook le pidió a Cambridge Analytica que eliminara los datos, el equipo de Facebook no tenía forma de corroborar que Cambridge Analytica cumpliera con su palabra, lo que pone en evidencia lo difícil que es hacer cumplir las políticas que efectivamente existen. En tercer lugar, si bien Facebook estaba al tanto del problema por lo menos desde diciembre del 2015, tardó mucho tiempo en avisar a los usuarios cuyos datos se habían visto comprometidos, y solo lo hizo después de la investigación periodística y el enorme escándalo público.

Ahora bien, el uso de la microsegmentación para hacer campañas políticas es particularmente problemático, ya que conlleva una falta de transparencia o control sobre los mensajes que se muestran y sobre quiénes los envían. Como consecuencia, los asesores detrás de estas campañas pueden usar anuncios políticos "oscuros" para enviar a los usuarios mensajes altamente personalizados que solo ellos pueden ver. A menudo, no queda claro qué organización o persona está detrás de esos mensajes, ni qué información están viendo y recibiendo otros usuarios.

Tras el escándalo de Cambridge Analytica, Google y Facebook han ajustado sus políticas con respecto a la publicidad de índole político[167] y han incorporado medidas orientadas a mejorar la transparencia en torno a quién paga por el espacio publicitario y bibliotecas de anuncios, que identifican anuncios sobre temas políticos. No obstante, según un análisis de Privacy International, al día de hoy, estas

161. Harry Davies, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, Guardian (RU), 11 de diciembre de 2015, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

162. Facebook, *Hard Questions: Update on Cambridge Analytica*, 21 de marzo de 2018, https://newsroom.fb.com/news/2018/03/hard-questions-cambridge-analytica

163. Paul Lewis, David Pegg y Alex Hern, *Cambridge Analytica kept Facebook data models through US election*, Guardian (RU), mayo de 2018, https://www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election

164. Matthew Rosenberg, Nicholas Confessore y Carole Cadwalladr, *2016 the Donald Trump Presidential campaign hired Cambridge Analytica*, New York Times, 17 de marzo de 2018; Carole Cadwalladr y Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,* Guardian (RU), 17 de marzo de 2018; CNBC, Facebook now lets you know if your data was shared with Cambridge Analytica, 9 de abril de 2018

165. Facebook, *An Update on Our App Developer Investigation*, 20 de septiembre de 2019, https://newsroom.fb.com/news/2019/09/an-update-on-our-app-developer-investigation/. Según la carta de respuesta enviada a Amnistía Internacional, que se incluye al final del informe, Facebook sostuvo lo siguiente: "La suspensión no indica necesariamente que estas aplicaciones presentaran una amenaza para los usuarios".

166. Facebook, *API Updates and Important Changes*, 25 de abril de 2019, https://developers.facebook.com/blog/post/2019/04/25/api-updates/

167. Google, *Introducing a new transparency report for political ads*, 15 de agosto de 2018, https://www.blog.google/technology/ads/introducing-new-transparency-report-political-ads/; Facebook, *A Better Way to Learn About Ads on Facebook*, 28 de marzo de 2019, https://newsroom.fb.com/news/2019/03/a-better-way-to-learn-about-ads/

medidas han resultado ineficaces y se han aplicado de manera irregular en diversos países. Por lo tanto, muchos usuarios de todas partes del mundo "carecen de información significativa sobre cómo se implementan los anuncios por segmentación en estas plataformas".[168] Otro análisis llevado a cabo por investigadores de Mozilla también detectó que la herramienta de Facebook es inadecuada.[169]

Básicamente, como el modelo de negocios depende de la elaboración de perfiles y la segmentación para insertar y presentar publicidad, las capacidades de estas plataformas seguirán siendo explotadas por terceros, incluso para llevar adelante campañas políticas.

MAXIMIZAR LA INTERACCIÓN

Las empresas tienen la responsabilidad de respetar la libertad de expresión, derecho que comprende la expresión que pudiera ser ofensiva o desagradable.[170] Por ejemplo, el Pacto Internacional de Derechos Civiles y Políticos exige que los estados prohíban únicamente "toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia". Muchas otras formas de expresión, incluso aquellas que causan indignación u ofensa, no pueden restringirse de manera legítima.

Sin embargo, el uso de algoritmos para seleccionar el contenido de las redes sociales y alentar a las personas a permanecer en la plataforma puede llevar a que Google y Facebook promuevan o amplíen el contenido abusivo, discriminatorio o de incitación al odio. Las plataformas recomiendan y promueven nuevo contenido basado en procesos algorítmicos no transparentes que determinan lo que más atrae a los usuarios.[171] Como hay más probabilidades de que las personas hagan clic en material sensacionalista o escandaloso, los llamados "motores de recomendación" de estas plataformas pueden llevar a los usuarios a lo que algunos han denominado una "madriguera de conejo" de contenido tóxico.[172]

La exdirectora de tecnología de Google, Nicole Wong, reconoce este problema ahora y declara: "La personalización de contenidos, la interacción... lo que te mantiene aquí, y que ahora conocemos muy bien. Es lo más indignante que existe".[173] Mark Zuckerberg sostuvo lo siguiente: "Nuestra investigación sugiere que, sin importar cuál sea el límite que marquemos para lo que está permitido, si hay contenido que se acerca a ese límite, las personas en promedio interactúan más con él, incluso cuando posteriormente nos dicen que no les gusta".[174]

Facebook sostiene que se enfoca "en la calidad del tiempo que los usuarios pasan en Facebook y no en la cantidad. El algoritmo de Facebook prioriza las publicaciones que, según las predicciones, darán lugar a *diálogos significativos*".[175] Sin embargo, incluso desde adentro de Facebook se admite la naturaleza intencionalmente adictiva del producto. Por ejemplo, Roger McNamee, quien fuera de los primeros inversores de Facebook y asesor de Mark Zuckerberg, escribió esto este mismo año: "el modelo de negocios depende de los anuncios, que, a su vez, dependen de la manipulación de la atención de los usuarios para que vean más anuncios. Una de las mejores maneras de manipular la atención es recurrir a la indignación y al miedo, emociones que aumentan la participación".[176]

168. Privacy International, *Social media companies have failed to provide adequate advertising transparency to users globally*, 3 de octubre de 2019, https://privacyinternational.org/long-read/3244/social-media-companies-have-failed-provide-adequate-advertising-transparency-users

169. Mozilla, *Facebook's Ad Archive API is Inadequate*, 29 de abril de 2019, https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadequate/

170. Comité de Derechos Humanos, *Observación general núm. 34, artículo 19: Libertad de opinión y libertad de expresión*, CCPR/C/GC/43, 12 de septiembre de 2011, párrafo 11.

171. Por ejemplo, Alex Madrigal, The Atlantic, *How YouTube's Algorithm Really Works*, noviembre de 2018 https://www.theatlantic.com/technology/archive/2018/11/how-youtubes-algorithm-really-works/575212/

172. Kevin Roose, *The Making of a YouTube Radical*, The New York Times, junio de 2019 https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html

173. Recode Decode, *Full Q&A: Former Google lawyer and deputy U.S. CTO Nicole Wong*, septiembre de 2018 https://www.vox.com/2018/9/12/17848384/nicole-wong-cto-lawyer-google-twitter-kara-swisher-decode-podcast-full-transcript

174. Mark Zuckerberg, *A Blueprint for Content Governance and Enforcement*, noviembre de 2018, https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/

175. Carta de Facebook a Amnistía Internacional. Ver anexo. La empresa también hace referencia a sus esfuerzos para reducir la viralización del discurso de odio y a otras medidas de moderación de contenidos.

176. Roger McNamee, *I Mentored Mark Zuckerberg. I Loved Facebook. But I Can't Stay Silent About What's Happening,* Time, 17 de enero de 2019, https://time.com/5505441/mark-zuckerberg-mentor-facebook-downfall/

El Relator Especial sobre la promoción y protección del derecho a la libertad de expresión ha señalado que "las aplicaciones de la inteligencia artificial a la búsqueda influyen enormemente en la difusión de conocimientos. Los recopiladores de contenidos y los sitios de noticias… eligen qué información mostrar a un individuo no en función de eventos importantes o recientes, sino con aplicaciones de inteligencia artificial que predicen los intereses de los usuarios y los patrones de noticias a partir de exhaustivos conjuntos de datos. Por lo tanto, la inteligencia artificial juega un papel importante, pero generalmente oculto, a la hora de darle forma a la información que los individuos consumen o incluso qué información saben que pueden consumir".[177] El Relator Especial también ha declarado que "en un sistema regido por la inteligencia artificial, la difusión de información e ideas es regida por fuerzas no transparentes con prioridades que pueden entrar en conflicto con un entorno favorable para la diversidad de los medios y las voces independientes".[178]

Por supuesto, el sensacionalismo en los medios no es un fenómeno nuevo, y no se limita a Internet. Pero los motores de recomendación de las redes sociales van mucho más allá del dicho "si hay sangre, vende": pueden privilegiar sistemáticamente el contenido extremo, como las teorías conspirativas, la misoginia y el racismo, para mantener a las personas en sus plataformas durante el mayor tiempo posible. Por ejemplo, un estudio académico sobre la propagación de sentimientos negativos hacia los refugiados en Facebook halló que "los crímenes de odio contra los refugiados aumentaron de manera desproporcionada en zonas con un mayor uso de Facebook durante períodos de gran hostilidad contra los refugiados en Internet".[179] De forma similar, se ha demostrado que los algoritmos detrás de la plataforma YouTube de Google tienen consecuencias perjudiciales diversas (ver cuadro abajo).

Además de privilegiar el contenido nocivo, los algoritmos de la plataforma también pueden atentar contra la libertad de expresión o llevar a la discriminación al censurar determinadas formas de contenido. Por ejemplo, las comunidades LGBTI han denunciado que los algoritmos de YouTube bloquean o censuran videos con contenido LGBTI al imponer automáticamente restricciones de edad y al "desmonetizar" los videos, es decir que les niegan a los productores cualquier tipo de ingresos por anuncios.[180] YouTube niega estas acusaciones y afirma que la empresa "no desmonetiza automáticamente el contenido LGBTQ".[11]

ESTUDIO DE CASO: EL ECOSISTEMA DE RADICALIZACIÓN DE YOUTUBE

Numerosos estudios de YouTube —realizados por el experto Zeynep Tufekci,[182] el exingeniero de YouTube Guillaume Chaslot,[183] The New York Times[184] y otros— han documentado que el algoritmo de recomendación de YouTube privilegia el contenido falso y escandaloso.

En teoría, tanto el acoso como las expresiones de odio violan las políticas de YouTube. En la práctica, el material que se acerca peligrosamente a esta línea (o la cruza) sigue disponible porque atrae mucha atención y es rentable para YouTube porque hace que las personas permanezcan en la plataforma durante más tiempo y, por lo tanto, que vean más anuncios, lo que, a su vez, le genera más ingresos a YouTube, que gana dinero con los anunciantes en función de la cantidad de vistas que obtiene un anuncio. Según la empresa, su sistema de recomendación algorítmica de nuevo

177. David Kaye, 2018, párrafo 11

178. David Kaye, 2018, párrafo 30

179. Karsten Müller y Carlo Schwarz, *Fanning the Flames of Hate: Social Media and Hate Crime,* University of Warwick, mayo de 2018, https://warwick.ac.uk/fac/soc/economics/research/centres/cage/manage/publications/373-2018_schwarz.pdf; Amanda Taub y Max Fisher, *Facebook Fueled Anti-Refugee Attacks in Germany, New Research Suggests*, New York Times, 21 de agosto de 2018

180. Julia Alexander, *LGBTQ YouTubers are suing YouTube over alleged discrimination*, The Verge, agosto de 2019 https://www.theverge.com/2019/8/14/20805283/lgbtq-youtuber-lawsuit-discrimination-alleged-video-recommendations-demonetization

181. Ibid.

182. Zeynep Tufekci, *YouTube, The Great Radicalizer*, The New York Times, marzo de 2018 https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.

183. El sitio de Chaslot, *Daily YouTube Recommendations*, hace un seguimiento de las recomendaciones de YouTube de más de mil canales. Ver https://algotransparency.org/. *Ver también How an ex-YouTube insider investigated its secret algorithm,* Guardian (RU), https://www.theguardian.com/technology/2018/feb/02/youtube-algorithm-election-clinton-trump-guillaume-chaslot.

184. Max Fisher y Amanda Taub, *How YouTube Radicalized Brazil*, New York Times, 11 de agosto de 2019, https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html

material es responsable del 70 % del tiempo total que las personas permanecen en la plataforma.[185]

Un informe de 2018 de una investigadora del grupo de expertos de Data & Society, Becca Lewis, describe cómo el motor de recomendación de YouTube monetiza el alcance y la "influencia" incluso para los que habitualmente profesan opiniones dañinas y racistas.[186]
En su estudio de 2018, *Alternative Influence: Broadcasting the Reactionary Right on YouTube*, Lewis esquematiza la red de *influencers* ultraderechistas en EE. UU. que utilizan el algoritmo de YouTube para beneficiarse de la desinformación y las expresiones de odio. La investigadora grafica cómo la combinación del algoritmo de recomendación de YouTube y las prácticas sociales de los YouTubers de ultraderecha crean un ecosistema de radicalización que logra que sea "sorprendentemente fácil que los usuarios queden expuestos a contenido cada vez más extremista".[187] Esto es especialmente problemático, escribe, dada la popularidad de YouTube entre los jóvenes como fuente de noticias.[188] Su conclusión: "Una enorme red de *influencers* en YouTube está transmitiendo ideas reaccionarias a los usuarios jóvenes y, en el proceso, los está radicalizando".[189]

El algoritmo también ayuda a reforzar la información falsa y los rumores. Al agrupar automáticamente diferentes videos que repiten la misma historia falsa, YouTube crea la ilusión de que hay más de una fuente para la misma idea. En la realidad, este aparente consenso es completamente fabricado por el algoritmo: de acuerdo con Debora Diniz, una activista por los derechos de la mujer que se convirtió en el blanco de una campaña de conspiración coordinada en Brasil, "parece como si el usuario hubiese hecho la conexión, pero es el sistema el que hace la conexión".[190] Estos problemas de sesgo de confirmación y sesgo de popularidad se han documentado en varias plataformas de redes sociales.[191]

En respuesta a algunos de estos informes, YouTube anunció —y no es la primera vez— cambios en la forma en que los algoritmos recomendarán contenido en la plataforma, pero hasta la fecha esos cambios solo afectan a un pequeño conjunto de videos en EE. UU.[192] La empresa continúa siendo objeto de una intensa crítica pública por permitir la monetización de contenido abusivo en su plataforma.[193] Sin embargo, la CEO de YouTube niega la acusación "de que dudamos en tomar medidas sobre el contenido problemático porque es beneficioso para nuestro negocio".[194] Google indicó que YouTube sigue trabajando para mejorar su función de recomendaciones.[195]

DISCRIMINACIÓN

Otro de los principales riesgos para los derechos que presentan la publicidad segmentada y la elaboración de perfiles, que constituyen las bases del modelo de negocios de Facebook y Google, es que ofrecer contenido dirigido a personas o grupos seleccionados puede fomentar la discriminación

185. Max Fisher y Amanda Taub, *How YouTube Radicalized Brazil*, New York Times, 11 de agosto de 2019

186. Rebecca Lewis, *Alternative Influence: Broadcasting the Reactionary Right on YouTube*, Data & Society, septiembre de 2018, https://datasociety.net/output/alternative-influence/

187. Ibid., p. 36

188. El informe cita un estudio de Pew Research Center donde se muestra que más del 90 % de los adultos entre 18 y 24 años utiliza YouTube: http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/pi_2018-03-01_social-media_0-01/.

189. Rebecca Lewis, https://twitter.com/beccalew/status/1042054175201185792

190. Max Fisher y Amanda Taub, *How YouTube Radicalized Brazil*, New York Times, 11 de agosto de 2019

191. Giovanni Luca Ciampaglia, Filippo Menczer, *Biases Make People Vulnerable to Misinformation Spread by Social Media*, The Conversation, 21 de junio de 2018 https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/

192. YouTube, *Continuing our work to improve recommendations on YouTube*, 25 de enero de 2019, https://youtube.googleblog.com/2019/01/continuing-our-work-to-improve.html

193. YouTube, *Taking a harder look at harassment*, 5 de junio de 2019 https://youtube.googleblog.com/2019/06/taking-harder-look-at-harassment.html

194. YouTube, *Susan Wojcicki: Preserving openness through responsibility*, agosto de 2019, https://youtube-creators.googleblog.com/2019/08/preserving-openness-through-responsibility.html

195. YouTube, *The Four Rs of Responsibility, Part 1: Removing harmful content*, 3 septiembre de 2019, https://youtube.googleblog.com/2019/09/the-four-rs-of-responsibility-remove.html

por parte de entidades privadas, o directamente por parte de las mismas plataformas, lo que socava el principio fundamental de que todas las personas deberían gozar de igual acceso a sus derechos humanos.[196] La no discriminación, junto con la igualdad ante la ley y la protección igual de la ley sin discriminación, conforman un principio básico y general relacionado con la protección de los derechos humanos.[197]

La elaboración de perfiles consiste de manera inherente en diferenciar a las personas a partir de sus características, creencias y comportamientos individuales. Se ha demostrado que la segmentación por parte de anunciantes y partidos políticos a través de las plataformas de Facebook y Google (es decir, cuando se decide incluir o excluir a ciertos grupos) ha implicado la elaboración de perfiles incluso con características sensibles, por ejemplo, en categorías como "menores de 18"[198], "afinidad multicultural"[199], "interés en el delito de traición a la patria"[200], "interés en [el exlíder Nazi] Joseph Goebbels"[201], "grupo con ingresos más bajos que el 198 %"[202], "interés en centros de tratamiento de la adicción"[203], "interés en el aborto"[204], "interés en el genocidio blanco"[205] u "orientación sexual"[206].

Las instancias individuales de uso de anuncios dirigidos no implica necesariamente una violación a los derechos de las personas: en muchos casos, cuando los anunciantes dirigen sus anuncios a los consumidores para venderles productos en función de sus intereses, no se están limitando derechos o libertades. Sin embargo, cuando se implementa en contextos que afectan de forma directa los derechos de las personas, incluidos sus derechos económicos, sociales y culturales, el hecho de que Facebook y Google posibiliten la segmentación granular para los anunciantes plantea intrínsecamente un alto riesgo de discriminación.

Desde hace tiempo, las políticas de anuncios de Facebook prohíben la discriminación.[207] Sin embargo, los periodistas de investigación demostraron que, durante años, Facebook les permitió a los anunciantes (para anuncios de viviendas, empleos y, lo que es más preocupante, partidos políticos) segmentar —y excluir— grupos en función de categorías protegidas como el origen étnico y la edad.[208] A principios de este año, Facebook se vio obligado a restringir el uso de la segmentación en anuncios de viviendas, empleo y créditos en los Estados Unidos, después de llegar a un acuerdo legal con asociaciones de derechos civiles.[209] Por ejemplo, los anunciantes ya no pueden dirigir anuncios sobre vivienda, empleo u oportunidades de crédito a personas según su edad, género, código postal o cualquier interés que describa características protegidas o que esté relacionado con estas

196. Chris Gillard, Friction-Free Racism, Real Life magazine, 15 de octubre de 2018, https://reallifemag.com/friction-free-racism/

197. Comité de Derechos Humanos, *Observación general núm. 18: No discriminación*, 10 de noviembre de 1989, párrafo 1.

198. Facebook, *Información sobre la segmentación basada en la edad,* https://www.facebook.com/help/103928676365132 ("La edad mínima permitida en Facebook es de 13 años, por lo que los anuncios deberán dirigirse a personas de esta edad o mayores").

199. ProPublica, *Facebook Promises to Bar Advertisers from Targeting Ads by Race or Ethnicity. Again.*, julio de 2018 https://www.propublica.org/article/facebook-promises-to-bar-advertisers-from-targeting-ads-by-race-or-ethnicity-again

200. Guardian (RU), *Facebook labels Russian users as 'interested in treason'*, julio de 2018, https://www.theguardian.com/technology/2018/jul/11/facebook-labels-russian-users-as-interested-in-treason

201. Los Angeles Times, *Facebook decided which users are interested in Nazis — and let advertisers target them directly*, febrero de 2019 https://www.latimes.com/business/technology/la-fi-tn-facebook-nazi-metal-ads-20190221-story.html

202. Google, *Acerca de la orientación demográfica*, https://support.google.com/google-ads/answer/2580383

203. En 2018, Facebook comenzó a limitar los anuncios de centros de tratamiento de la adicción a organizaciones certificadas, pero solo en EE. UU. Ver Facebook, *Restricting Ads for Addiction Treatment Centers and Bail Bonds*, 9 de agosto de 2018, https://www.facebook.com/business/news/restricting-ads-for-addiction-treatment-centers-and-bail-bonds

204. Políticas de Google Ads, Cuidado de la salud y medicamentos, https://support.google.com/adspolicy/answer/176031 (Esta categoría no está disponible en varios países).

205. The Intercept, *Facebook Allowed Advertisers to Target Users Interested in "White Genocide" — Even in Wake of Pittsburgh Massacre*, *disponible en* https://theintercept.com/2018/11/02/facebook-ads-white-supremacy-pittsburgh-shooting/. Desde entonces, esta categoría se ha desactivado.

206. La posibilidad de mostrar anuncios a los usuarios de Facebook en función de la orientación sexual estuvo disponible hasta febrero de 2019. Buzzfeed, *Facebook Has Blocked Ad Targeting By Sexual Orientation*, 21 de marzo de 2018 https://www.buzzfeednews.com/article/alexkantrowitz/facebook-has-blocked-ad-targeting-by-sexual-orientation.

207. Política de publicidad de Facebook, *Contenido prohibido: Prácticas discriminatorias*, https://www.facebook.com/policies/ads/prohibited_content/discriminatory_practices

208. Julia Angwin y Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race*, 28 de octubre de 2016 https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

209. Facebook, *Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising*, 19 de marzo de 2019, https://newsroom.fb.com/news/2019/03/protecting-against-discrimination-in-ads; ACLU, Summary Of Settlements Between Civil Rights Advocates And Facebook, 19 de marzo de 2019, https://www.aclu.org/other/summary-settlements-between-civil-rights-advocates-and-facebook

características. Sin embargo, estas medidas solo afectan a los anunciantes con sede en EE. UU. o que se dirigen a personas en EE. UU., lo que quiere decir que las personas del resto del mundo todavía corren el riesgo de ser discriminadas en estas áreas.

Cabe destacar que, además del riesgo de discriminación por el uso de terceros de las capacidades de lanzar anuncios dirigidos que tienen las empresas, los sistemas algorítmicos que determinan concretamente cómo se *muestran* los anuncios en las plataformas pueden tener consecuencias discriminatorias, incluso cuando los anunciantes mismos segmentan los anuncios de un modo neutral.[210] Esto aumenta el riesgo de que las empresas puedan generar discriminación de forma directa a través de la forma en que sus sistemas algorítmicos se optimizan para lanzar anuncios, p. ej., de acuerdo con la "relevancia" o los usuarios más "valiosos". En marzo de 2019, el Departamento de Vivienda y Desarrollo Urbano de los Estados Unidos (HUD) demandó a Facebook por discriminación en materia de vivienda, lo que incluía discriminación a través de su propio sistema de distribución de anuncios, y señaló que los mecanismos de Facebook "funcionan igual que un anunciante que intencionalmente dirige anuncios o excluye a usuarios en función de que pertenecen a una categoría protegida".[211] En su respuesta, Facebook cuestionó esta afirmación y sostuvo: "el HUD no tenía pruebas de que nuestros sistemas de IA discriminaran a las personas".[212] Según lo que se sabe, el HUD también estaría investigando las prácticas de anuncios de Google y Twitter.[213]

210. Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, Aaron Rieke, *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*, abril de 2019, https://arxiv.org/abs/1904.02095; Carnegie Mellon University, *Questioning the Fairness of Targeting Ads Online*, julio de 2015, https://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html

211. Departamento de Vivienda y Desarrollo Urbano de los Estados Unidos contra Facebook, Acusación por discriminación, 28 de marzo de 2019, https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf

212. Declaración de Facebook en ProPublica, *HUD Sues Facebook Over Housing Discrimination and Says the Company's Algorithms Have Made the Problem Worse*, marzo de 2019, https://www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms

213. Washington Post, *HUD is reviewing Twitter's and Google's ad practices as part of housing discrimination probe*, 28 de marzo de 2019, https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/

4. LA CONCENTRACIÓN DE PODER, UNA BARRERA CONTRA LA RESPONSABILIZACIÓN

> ***"El mundo del software, especialmente para las plataformas, es un mercado en el que el ganador se lleva todo".***
>
> Bill Gates, cofundador de Microsoft.[214]

El modelo de negocios basado en la vigilancia que aplican Google y Facebook les ha permitido obtener el control casi total de los principales canales a través de los cuales la mayoría de las personas interactúa en el mundo digital y en la "plaza pública" global, y esto los ha convertido en potencias de proporciones históricas. Nunca antes una empresa había podido arbitrar y clasificar la transmisión de información a más de dos mil millones de usuarios en múltiples países.

El poder concentrado de las empresas es multifacético. Paul Nemitz, asesor principal de la Comisión Europea, ha establecido que la singular concentración de poder en manos de las grandes empresas tecnológicas consiste en cuatro elementos clave, que deben considerarse como conjunto y en suma: el poder del dinero, que les permite influir en la política y los mercados; el poder sobre las infraestructuras de la democracia y el discurso; el poder sobre los individuos a partir de la elaboración de perfiles y la capacidad de aprovechar ese conocimiento para sus propios intereses, y el poder hegemónico en la innovación en IA.[215]

Este poder concentrado va de la mano del impacto respecto de los derechos humanos que tiene el modelo de negocios; de hecho, uno ha impulsado al otro simbióticamente. El derecho a la privacidad en Internet se ha visto socavado en gran parte porque los servicios básicos de Internet pasaron a ser controlados por empresas que dependen de la vigilancia. A su vez, las empresas lograron establecer este poder hegemónico porque priorizaron las ganancias obtenidas con la publicidad por sobre la privacidad y otros derechos.

214. The Verge, *Bill Gates says his 'greatest mistake ever' was Microsoft losing to Android*, junio de 2019

215. Paul Nemitz, asesor principal de la Comisión Europea (escrito a título personal), *Constitutional democracy and technology in the age of artificial intelligence*, octubre de 2018. El análisis se refiere al poder de Google, Facebook, Microsoft, Apple y Amazon.

Este poder de las plataformas no solo ha exacerbado e incrementado su impacto respecto de los derechos, sino que además ha generado una situación en la que resulta muy difícil responsabilizar a las empresas o que los individuos afectados puedan acceder a una reparación adecuada.

ACCESO A INTERNET A COSTA DE LA VIGILANCIA

El acceso a Internet se considera desde hace tiempo un facilitador esencial del ejercicio de los derechos humanos en la era digital. En 2011, el Relator Especial de la ONU sobre libertad de expresión reconoció que "la naturaleza singular y transformadora de Internet les permite a las personas ejercer no solo su derecho a la libertad de opinión y expresión, sino también muchos otros derechos humanos, y ofrece la posibilidad de impulsar progresos en la sociedad en su conjunto".[216] En 2016, el Consejo de Derechos Humanos de la ONU destacó la importancia de "aplicar un enfoque integral basado en los derechos humanos al proporcionar y ampliar el acceso a Internet, y de que Internet sea abierta, accesible y nutrida".[217]

La función de Google y Facebook como "guardianes" del mundo digital (que se describe en el capítulo 1) implica que ejercen una influencia importante respecto del disfrute de los derechos humanos en Internet; de hecho, la gran mayoría de los usuarios de Internet dependen de los servicios que estas empresas prestan. De esta forma, las plataformas se han vuelto esenciales para la forma en que las personas ejercen sus derechos humanos en Internet, y a diario facilitan el ejercicio de la libertad de expresión, los derechos de reunión pacífica y de asociación y otros derechos.[218]

A su vez, el poder hegemónico de las plataformas de estas empresas implica que actualmente es imposible interactuar en Internet sin "aceptar" su modelo de negocios basado en la vigilancia. Debido al "efecto de red" (que se describen posteriormente), no es realista pensar que las personas pueden abandonar las redes sociales donde se encuentran todos sus amigos y familiares. Las personas que se registraron en plataformas que respetaban mucho más su privacidad (ver a continuación) —o antes de que estas fueran adquiridas por Google o Facebook— ahora se enfrentan a la falsa posibilidad de elegir: pueden dejar un servicio del que dependen o pueden someterse a la vigilancia. En algunos países del mundo, Facebook se asocia directamente al acceso a Internet, y, a nivel mundial, una inmensa mayoría de *smartphones* utiliza el sistema operativo Android de Google. Incluso para las personas que no se han suscrito a ninguno de sus servicios es extremadamente difícil utilizar Internet sin someterse a la recolección por parte de datos de ambas empresas.[219]

Esto ha generado una situación paradójica en la que, para poder acceder a Internet y disfrutar de sus derechos humanos allí, las personas se ven obligadas a someterse a un sistema que se basa en la injerencia en el derecho a la privacidad a una escala sin precedentes, con un impacto proporcional respecto de otros derechos humanos, incluidos los derechos a la libertad de expresión y a la no discriminación. Esta situación se contradice totalmente con la afirmación del Consejo de Derechos Humanos sobre la importancia de que "se aplique un enfoque basado en los derechos humanos para facilitar y ampliar el acceso a Internet".[220] En junio de 2019, un grupo de expertos de la ONU también expresó que "el espacio digital no es un espacio neutral. A nivel de arquitectura física, reglamentación y uso, diferentes grupos imponen sus intereses en él. Sin embargo, los principios del derecho internacional de los derechos humanos deberían ser la base central de su desarrollo".[221]

---

216. Frank La Rue, Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, informe presentado ante el Consejo de Derechos Humanos de la ONU, 16 de mayo de 2011, documento A/HRC/17/27

217. Consejo de Derechos Humanos de la ONU, *Promoción, protección y disfrute de los derechos humanos en Internet*, junio de 2016, documento A/HRC/32/L.20

218. "En la era digital, el ejercicio de los derechos a la libertad de reunión pacífica y de asociación ha pasado a depender, en gran medida, de empresas, cuyas obligaciones jurídicas, políticas, normativa técnica, modelo económico y algoritmos pueden afectar a esas libertades". Clément Nyaletsossi Voule, Relator Especial sobre el derecho a la libertad de reunión pacífica y de asociación

219. Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2014; Kashmir Hill, *Goodbye Big Five*, Gizmodo, enero de 2019

220. Consejo de Derechos Humanos de la ONU, *Promoción, protección y disfrute de los derechos humanos en Internet*, junio de 2016, documento A/HRC/32/L.20

221. ACNUDH, *UN experts stress links between digital space and human rights at RightsCon, Tunis,* 13 de junio de 2019 www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24696

LA CONCENTRACIÓN DE PODER AGRAVA EL DAÑO

El creciente poder de Google y Facebook como controladores de las formas en las que las personas interactúan con el mundo digital ha sido un factor clave en la erosión de la privacidad en Internet. Diversos análisis que trazan el ascenso del poder hegemónico de Google y Facebook muestran que las empresas lograron incrementar en gran medida la amplitud y la profundidad de su vigilancia de forma paralela a su control sobre los principales canales de Internet y a la disminución de alternativas relevantes.[222]

Originalmente, cuando operaban en mercados altamente competitivos, tanto Google como Facebook no condicionaban el acceso a sus servicios a la vigilancia omnipresente. La política de privacidad inicial de Facebook declaraba: "No usamos ni usaremos cookies para recopilar información privada de ningún usuario".[223] La primera política de privacidad de Google establecía que la empresa compartía información sobre los usuarios con los anunciantes, pero aclaraba: "solo nos referimos a nuestros usuarios en conjunto, no como individuos". Esto se contradice de forma directa con el modelo actual de publicidad dirigida y altamente personalizada.[224]

La transformación de las empresas desde sus comienzos, cuando respetaban más la privacidad, hasta su modelo de negocios actual de vigilancia omnipresente ha sido gradual. Google dio el paso final para adoptar plenamente el modelo basado en la vigilancia en 2016, cuando cambió su política de privacidad para poder combinar datos de su red publicitaria DoubleClick (desde entonces rebautizada como Google Marketing Platform) con datos personales recopilados desde sus otras plataformas.[225] Esto significó que la empresa pudiera dirigir de forma directa los anuncios a individuos identificables, a partir de información sumamente personal. En respuesta, la periodista especializada en privacidad de datos Julia Angwin declaró que Google había "borrado silenciosamente el límite en cuanto a la privacidad".[226] Facebook ya había tomado una medida similar en 2014, cuando anunció que utilizaría datos de navegación web a los fines de la publicidad dirigida.[227]

Las empresas pudieron dar este paso final porque ya habían establecido su poder hegemónico. Como lo demuestran los modelos de negocios iniciales de las empresas, en un mercado competitivo, los usuarios de Internet no tolerarían semejante nivel de intrusión en su privacidad y se cambiarían a servicios alternativos. Actualmente, las empresas pueden darse el lujo de abusar de la privacidad, porque las personas no tienen más remedio que aceptarlo.[228]

LAS VULNERACIONES DE DERECHOS HUMANOS ALIMENTAN LA CONCENTRACIÓN DE PODER

A su vez, el modelo de negocios basado en la vigilancia tiende inherentemente a aumentar de manera exponencial el poder y la magnitud de las plataformas, por lo que el abuso de la privacidad y de otros derechos también ha ayudado a concentrar el poder en manos de Google y Facebook. La extracción de más y más datos les ha permitido a las empresas ganar mayor control sobre las principales

222. Ver, por ejemplo, Zuboff, 2018; Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy,* 16 Berkeley Bus. L.J. 39, 2019

223. Facebook, *The Facebook Privacy Policy (2004),* citado por Dra. Liza Lovdahl Gormsen y Dr. Jose Tomas Llanos, *Facebook's Anticompetitive Lean in Strategies,* junio de 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3400204 (Gormsen y Llanos, 2019)

224. Google, Política de privacidad, junio de 1999, https://policies.google.com/privacy/archive/19990609?hl=en&gl=ZZ

225. Google, Política de privacidad, junio de 2016, https://policies.google.com/privacy/archive/20160325-20160628?hl=en&gl=ZZ

226. Julia Angwin, *Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking*, ProPublica, 21 de octubre de 2016, https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking

227. AdAge, *Facebook To Use Web Browsing History For Ad Targeting*, junio de 2014, https://adage.com/article/digital/facebook-web-browsing-history-ad-targeting/293656

228. "Las plataformas de comunicación en Internet… pueden compararse con los servicios públicos en el sentido de que los usuarios sienten que no pueden vivir sin ellas y, por lo tanto, no tienen otra opción más que aceptar sus términos de servicio. En este momento, los proveedores de estos servicios tienen poco incentivo para responder a las inquietudes sobre el uso indebido de los datos o el daño que causan en Internet, e incluso el daño que le provocan a la sociedad", Comité Selecto de la Cámara de los Lores del Reino Unido sobre las comunicaciones, *Regulating in a Digital World*, marzo de 2019, párrafo 45 Facebook cuestionó esta conclusión y sostuvo que "por el contrario; sabemos que si no protegemos los datos de las personas, perderemos su confianza". Ver la respuesta de Facebook a Amnistía Internacional en el anexo que se incluye.

maneras en las que las personas interactúan con Internet, en una medida que probablemente no habría sido posible si las empresas hubiesen implementado un modelo con más respeto hacia la privacidad.

En primer lugar, existe un fenómeno económico conocido como "efecto de red": cuantos más usuarios tiene la plataforma, más valiosa se vuelve, tanto para los usuarios mismos como para otros. Las plataformas en Internet —y el modelo de negocio detrás de ellas— son por naturaleza propensas a estos efectos de red. Muchos usuarios se unen a Facebook porque sus amigos usan Facebook; los anunciantes corren hacia YouTube porque tiene la audiencia más grande. Esto tiene un efecto dominó: cuanto más grande se vuelve la red o la plataforma, más dependen de ellas las personas, y más se consolida su posición, por lo que a los usuarios les cuesta abandonar la plataforma y a los competidores les cuesta imponer una alternativa.

La extracción y el análisis de datos de este modelo de negocios también generan un efecto de red relacionado con datos específicos.[229] La acumulación de una mayor cantidad de datos le permite a una empresa entrenar mejor a los modelos de aprendizaje automático y a los algoritmos que realizan predicciones sobre el comportamiento. A su vez, estas funciones predictivas se implementan para mantener a las personas en la plataforma y así obtener más datos y conservar el control sobre los flujos de datos. La optimización de las funciones predictivas también lleva a una mayor ganancia publicitaria, ya que aumenta el valor de la plataforma y el poder de la empresa en el mercado.

Los ciclos de retroalimentación de este sistema, combinados con los efectos de red tradicionales, han sido determinantes en la rápida expansión de la escala y el impacto de las plataformas, y, por lo tanto, en la concentración de poder en manos de Google y Facebook en el mundo digital. Durante nuestra rápida transición hacia un mundo donde la "Internet de las cosas", el análisis de datos y la inteligencia artificial conforman el núcleo de la economía, las bóvedas de datos de Google y Facebook y su control sobre la más avanzada tecnología de aprendizaje automático e inteligencia artificial reforzarán aún más su posición. Los marcos de aprendizaje automático respaldados por Google y Facebook —TensorFlow y PyTorch, respectivamente— se han convertido en las principales herramientas para los desarrolladores de inteligencia artificial.[230]

Las empresas también han logrado aprovechar sus ventajas obtenidas a partir de los datos —y la influencia económica que va de la mano— para evitar el desarrollo de servicios alternativos. Lo hacen mediante varios métodos: "conectando" un servicio al otro, aprovechando su poder en un área para intentar aumentar su poder en otra;[231] bajando de categoría a los servicios ofrecidos por potenciales competidores en sus propias plataformas (p. ej., en los resultados de búsqueda),[232] y sofocando a las empresas que ofrecen servicios similares o que constituyen una competencia potencial al copiar o directamente comprar la empresa.[233] Este patrón se ha vuelto tan conocido que los inversores de capital riesgo en Silicon Valley dicen que Google y Facebook han creado una "zona de muerte":[234] un área económica donde un competidor no puede echar raíces y donde el único modelo de negocios viable para una empresa nueva en el mercado es ser adquirida por Google o Facebook.

229. Gormsen y Llanos, 2019

230. Jeff Hale, *Which Deep Learning Framework is Growing Fastest?,* KDnuggets, abril de 2019, https://www.kdnuggets.com/2019/05/which-deep-learning-framework-growing-fastest.html

231. Comisión Europea, *Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine,* 18 de julio de 2018, http://europa.eu/rapid/press-release_IP-18-4581_en.htm

232. Comisión Europea, *Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service,* 27 de junio de 2017, http://europa.eu/rapid/press-release_IP-17-1784_en.htm. Ver también *The Case Against Google*, The New York Times, 20 de febrero de 2018, www.nytimes.com/2018/02/20/magazine/the-case-against-google.html

233. Ver, por ejemplo, Wired, If you can't build it, buy it: *Google's biggest acquisitions mapped,* septiembre de 2017; Billy Gallagher, *Copycat: How Facebook Tried to Squash Snapchat,* Wired, febrero de 2018; New York Post, *Facebook boasted of buying Instagram to kill the competition: sources*, febrero de 2019

234. The Economist, *American tech giants are making life tough for startups*, 2 de junio de 2018

LA CONCENTRACIÓN DE PODER, UNA BARRERA CONTRA LA RESPONSABILIZACIÓN

El desequilibrio entre el poder multifacético de las grandes empresas de tecnología como Google y Facebook, como se describió anteriormente, y la capacidad de los gobiernos para regularlo de forma sustancial es un excelente ejemplo de las "brechas de gobernanza" entre "el alcance y el impacto de las fuerzas y los actores económicos, y la capacidad que tienen las sociedades para afrontar las consecuencias adversas". John Ruggie, Representante Especial de la ONU para las Empresas y los Derechos Humanos, identificó esas brechas como la "causa raíz" del desafío mundial empresarial y de derechos humanos provocado por la globalización.[235]

La gran acumulación de datos detallados por parte de Google y Facebook mediante el control de plataformas y servicios que están profundamente incorporados en casi todos los aspectos de la vida moderna ha creado enormes asimetrías de información entre las empresas por un lado y los gobiernos y los usuarios de Internet por el otro. Zuboff explica que "el capital de vigilancia privado ha institucionalizado las asimetrías de conocimiento como nunca antes se ha visto en la historia de la humanidad. Saben todo sobre nosotros; y no sabemos casi nada de ellos".[236]

La velocidad a la que han crecido las plataformas de Google y Facebook hasta alcanzar una escala inmensa y operar en distintas jurisdicciones demuestra que los Estados no han logrado establecer normas al mismo ritmo al que se incrementó el impacto de las empresas respecto de los derechos de las personas.[237] En la actualidad, hay ejecutivos de Silicon Valley que reconocen públicamente la brecha. Brad Smith, CEO de Microsoft, declaró: "La tecnología digital es casi la única tecnología que ha estado tan desregulada por tanto tiempo".[238] Mark Zuckerberg pidió que "los gobiernos y las autoridades reguladoras tengan un papel más activo" en términos generales y también en los temas relacionados con la privacidad de datos.[239] En 2014, Eric Schmidt, el ex CEO de Google, y Jared Cohen, quien fuera en el momento el director de Google Ideas, afirmaron que el "universo cibernético es el espacio desregulado más grande del mundo".[240] Incluso desde Google se declaró que es "evidente que los marcos legales internacionales están quedando desactualizados en comparación con la innovación tecnológica".[241]

A pesar de que las autoridades en materia impositiva y de protección y regulación de la competencia de todo el mundo han implementado numerosas medidas regulatorias en contra de las grandes empresas de tecnología, al día de hoy, ninguna medida ha logrado convulsionar realmente a los impulsores principales del modelo de negocios basado en la vigilancia.

A modo de ejemplo destacado, en junio de 2019, la Comisión Federal de Comercio de Estados Unidos le aplicó a Facebook una sanción récord de US$ 5000 millones y le impuso una variedad de nuevos requisitos de privacidad luego de una investigación que se realizó a raíz del escándalo de Cambridge Analytica.[242] Aunque la multa es la acción coercitiva más grande de la que se tenga registro, sigue siendo relativamente insignificante en comparación con las ganancias y los ingresos anuales de la empresa, lo que se ve ilustrado por el hecho de que, luego de que se anunciara la multa,

---

235. John Ruggie, Representante Especial de la ONU para la problemática de los derechos humanos y las corporaciones transnacionales y otras empresas, Informe para el Consejo de Derechos Humanos, abril de 2008, A/HRC/8/5

236. https://www.democracynow.org/2019/3/1/age_of_surveillance_capitalism_we_thought

237. Ver, p. ej., Comité sobre Comunicación de la Cámara de los Lores del Reino Unido, *Regulating in a Digital World,* marzo de 2019: "la regulación del universo cibernético no le ha seguido el ritmo a la función que cumple en nuestra vida"; Deloitte Insights, *The future of regulation*, junio de 2018, https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html; Daniel Malan, *The law can't keep up with new tech. Here's how to close the gap,* Foro Económico Mundial, junio de 2018, https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up

238. NPR, *Microsoft President: Democracy Is At Stake. Regulate Big Tech,* septiembre de 2019

239. Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas,* Washington Post, marzo de 2019

240. Schmidt and Cohen, *The New Digital Age,* 2014,

241. Google, presentación para la oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre el derecho a la privacidad en la era digital, 2018

242. Comisión Federal de Comercio de Estados Unidos, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, 24 de julio de 2019, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

el precio de las acciones de Facebook subió.[243] Cabe destacar que el acuerdo no cuestionó el modelo subyacente de vigilancia permanente y de creación de perfiles conductuales para el uso de anuncios dirigidos. Rohit Chopra, Comisionado de Comercio de Estados Unidos, sostuvo lo siguiente en su voto en disidencia: "El acuerdo no impone ningún cambio significativo a la estructura de la empresa ni a los incentivos financieros, elementos que llevaron a esas infracciones. Tampoco incluye restricciones respecto de las tácticas de publicidad o vigilancia masiva de la empresa".[244]

Sin embargo, los vientos están cambiando: cada vez hay más interés por parte de las autoridades regulatorias y los legisladores de varias jurisdicciones en enfrentar el poder hegemónico de Google y Facebook, principalmente por medio de leyes de protección de datos y de la competencia.

Google y Facebook están recibiendo un aluvión de demandas desde que entró en vigencia el RGPD de la Unión Europea. La Comisión de Protección de Datos de Irlanda, donde Google y Facebook tienen sus sedes centrales europeas, tiene varias investigaciones en curso de ambas empresas, incluida una relacionada con la publicidad orientada y el análisis conductual.[245] En enero de 2019, el órgano que controla la protección de datos en Francia impuso una multa récord de 50 millones de euros a Google por varias infracciones, entre las que se incluía la falta de consentimiento válido en relación con la personalización de anuncios.[246]

En EE. UU., tanto Google como Facebook son objeto de varias investigaciones antimonopolio que llevan a cabo el Departamento de Justicia, la Comisión Federal de Comercio, el Subcomité Judicial de la Cámara de Representantes y dos grupos distintos de fiscales generales, entre otros.[247] Por otra parte, en 2018, California aprobó la ley de confidencialidad más progresista de Estados Unidos, la Ley de confidencialidad para el consumidor de California (CCPA, por su sigla en inglés), que otorga a los residentes de ese estado nuevos derechos para conocer qué información personal recopilan y comparten las empresas y rechazar la venta de esos datos.[248]

En septiembre de 2019, fue reelecta la Comisaria europea de la Competencia Margrethe Vestager, quien asumió su puesto con una cartera ampliada sobre regulaciones y políticas digitales,[249] lo que indica una declaración de intención en torno a la regulación de las grandes empresas de tecnología como consecuencia de varios fallos importantes de la Comisión en materia de monopolios en contra de empresas de Silicon Valley.[250] Esta ola no solo tiene lugar en Estados Unidos y la Unión Europea: la comisión de la competencia de Australia publicó un informe importante sobre cómo enfrentar el poder de Google y Facebook. Además, las autoridades que regulan la competencia en cuatro de los cinco países del BRICS emitieron un informe inicial que evalúa los mercados digitales.[251]

La autoridad alemana de regulación de la competencia emitió una decisión emblemática en febrero de 2019 que sirve de ejemplo de cómo un enfoque articulado entre competencia y protección de datos podría afectar los incentivos fundamentales del modelo de negocios basado en la vigilancia. El fallo prohíbe que Facebook combine datos entre sus distintas plataformas, como Instagram y WhatsApp, sin consentimiento, lo que pone directamente en jaque la posibilidad de la empresa de aprovecharse

243. MIT Technology Review, *Facebook is actually worth more thanks to news of the FTC's $5 billion fine,* 15 de julio de 2019

244. FTC, *Dissenting Statement Of Commissioner Rohit Chopra*, In re Facebook, Inc. Expediente de la Comisión nro. 1823109, 24 de julio de 2019

245. Ver Informe anual del 25 de mayo al 31 de diciembre de 2018 de la Comisión de Protección de Datos, Multinational Technology Companies Statutory Inquiries commenced, p. 50; *Data Protection Commission opens statutory inquiry into Google Ireland Limited*, mayo de 2019 https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited

246. Commission Nationale de l'Informatique et des Libertés (CNIL), *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, 21 de enero de 2019. Google ha apelado la decisión.

247. Marcy Gordon y Matt O'Brien, Associated Press, *As feds loom, states hit Facebook, Google with new probes*, 6 de septiembre de 2019, https://www.apnews.com/5d4d10e28b4841c8a3a723095d4c0d16

248. Ley de confidencialidad para el consumidor de California (CCPA), 2018, https://oag.ca.gov/privacy/ccpa

249. Wall Street Journal, *EU Commissioner Who Targeted Tech Giants Gets Second Term,* 10 de septiembre de 2019

250. Por ejemplo, la comisión sancionó a Google con una multa de 4340 millones de euros por el uso ilegal del sistema operativo Android para "fortalecer el dominio de su motor de búsqueda" y con otra de 1490 millones de euros por "el abuso de su posición dominante" en la publicidad en búsquedas en línea. Google ha apelado ambos fallos.

251. Comisión Australiana de la Competencia y del Consumidor, *Holistic, dynamic reforms needed to address dominance of digital platforms,* 26 de julio de 2019, https://www.accc.gov.au/media-release/holistic-dynamic-reforms-needed-to-address-dominance-of-digital-platforms; Consejo Administrativo de Defensa Económica (CADE) de Brasil, *Cade releases report on digital economy*, septiembre de 2019, http://www.cade.gov.br/cade_english/press-releases/cade-releases-report-on-digital-economy-during-the-vi-brics-competition-conference

de su control sobre esas plataformas.[252] No obstante, un tribunal regional suspendió la implementación del fallo a raíz de la apelación de Facebook.[253]

Esa tendencia indica que es posible que la era de la autorregulación de las grandes empresas tecnológicas esté llegando a su fin. Y es muy probable que una combinación de acciones coercitivas y legislación nueva lleven a una mayor supervisión gubernamental de las empresas de tecnología. Esas iniciativas podrían garantizar que Google y Facebook cumplan con su responsabilidad de respetar los derechos humanos. Sin embargo, los gobiernos deben asegurarse de que las regulaciones futuras del sector de la tecnología estén alineadas con la obligación del Estado en virtud del derecho internacional de proteger a las personas y a las comunidades de las actividades perjudiciales de los agentes corporativos, por ejemplo, mediante "políticas adecuadas, actividades de reglamentación y sometimiento a la justicia".[254]

LOBBY CORPORATIVO

Google y Facebook han buscado debilitar la regulación de varias formas, por ejemplo, usando sus recursos para realizar un gran lobby corporativo. Es importante resaltar que las iniciativas de lobby de las empresas abarcan una amplia variedad de otros asuntos empresariales y no todo el dinero que gastan Google y Facebook en hacer lobby tiene un impacto en los derechos humanos. Sin embargo, las exorbitantes cifras que gastan las empresas en lobby sirven para ilustrar su poder e influencia política. Por ejemplo, Google gastó más de 8 millones de euros en hacer lobby en la Unión Europea en 2018, mientras que Facebook gastó más de 3,5 millones de euros.[255] Para poner esos datos en perspectiva, Google gastó más dinero que cualquier otra empresa para hacer lobby en la Unión Europea ese año, seguida por Microsoft, Shell y Facebook.[256] Google y Facebook participaron activamente del lobby en contra del Reglamento General de Protección de Datos (GDPR) de Europa, que entró en vigencia para todos los estados miembro de la Unión Europea en 2018.[257]

Y esas empresas gastan aún más dinero para hacer lobby ante el gobierno de Estados Unidos. Center for Responsive Politics, una organización sin fines de lucro ni afiliación política que rastrea el gasto en actividades de lobby en Estados Unidos, sostiene que Google gastó US$ 21,2 millones para hacer lobby en el gobierno estadounidense en 2018 (un aumento del 17,6 % en comparación con el año anterior), mientras que Facebook gastó US$ 12,6 millones (un aumento de 9,6 % en comparación con el año anterior).[258] Además, las empresas de tecnología financian una amplia variedad de centros de investigación para reforzar sus argumentos.[259] Estas empresas hacen lobby tanto para evitar posibles medidas antimonopolio como para promover posibles leyes federales con el objetivo de anular leyes de confidencialidad más exigentes que están vigentes a nivel estatal. También se resisten fervientemente a esas

252. Oficina de defensa de la competencia de Alemania (Bundeskartellamt), *Bundeskartellamt prohibits Facebook from combining user data from different sources: Background information,* 7 de febrero de 2019, https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf

253. Herbert Smith Freehills, *German FCO's landmark Facebook decision suspended on appeal*, 27 de agosto 2019, https://hsfnotes.com/crt/2019/08/27/german-fcos-landmark-facebook-decision-suspended-on-appeal

254. Principios rectores sobre las empresas y los derechos humanos de la ONU, principio rector 1

255. Ver el perfil de Google del Registro de transparencia de la Unión Europea, http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=03181945560-59; y el perfil de Facebook, http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=28666427835-74

256. Statista, *The companies spending the most on EU lobbying,* 29 de abril de 2019, https://www.msn.com/en-us/finance/news/the-companies-spending-the-most-on-eu-lobbying/ar-BBWoSWM

257. Ver, p. ej. Laura Kayali, *Inside Facebook's fight against European regulation*, Politico, 23 de enero de 2019, https://www.politico.eu/article/inside-story-facebook-fight-against-european-regulation/

258. Ver los perfiles de empresas que hacen lobby creados por The Center for Responsive Politics: Google, https://www.opensecrets.org/lobby/firmsum.php?id=D000022008&year=2018; Facebook, https://www.opensecrets.org/lobby/clientsum.php?id=D000033563&year=2018

259. Lee Fang, *Silicon Valley-funded privacy think tanks fight in DC to unravel state-level consumer privacy protections,* The Intercept, 16 de abril de 2019, en: https://theintercept.com/2019/04/16/consumer-privacy-laws-california/

iniciativas a nivel estatal, incluidas la Ley de confidencialidad para el consumidor de California y la Ley de confidencialidad de datos biométricos de Illinois.[260]

Por último, el lobby no se limita solo a Europa y a Estados Unidos. Según The Guardian, unos documentos de Facebook que se filtraron a principios de año revelaron "una operación secreta de lobby global orientada a cientos de legisladores y autoridades reguladoras con el objetivo de generar influencia en todo el mundo, incluidos países como el Reino Unido, Estados Unidos, Canadá, India, Vietnam, Argentina, Brasil, Malasia y los 28 estados de la Unión Europea".[262]

En su respuesta a este informe, Google destacó la transparencia de los fondos que otorga a terceros y la información que publica sobre sus actividades de lobby.[263] Facebook declaró que cumple todas las leyes y directivas aplicables cuando lleva a cabo actividades de lobby.[264]

OBSTÁCULOS EN LA BÚSQUEDA DE REPARACIÓN

La escala de las plataformas como Google y Facebook también crea algunos obstáculos particulares para las personas a la hora de buscar y obtener una reparación efectiva después de sufrir el impacto negativo del modelo de negocios basado en la vigilancia respecto de sus derechos humanos.[265]

En parte, eso se debe a los desafíos inherentes que presentan los sistemas algorítmicos a la hora de obtener una reparación.

Un problema importante es la falta de aplicación efectiva de la reglamentación de protección de datos vigente. Incluso en Europa, que tiene un sistema de protección de datos relativamente sólido, las autoridades reguladoras no cuentan con los recursos ni la experiencia para investigar las violaciones al reglamento y llevar a los responsables ante la justicia de manera adecuada.[266] Asimismo, las acciones privadas iniciadas por personas físicas son poco comunes debido a la "falta de conocimiento de los derechos, los procedimientos engorrosos, los costos de justicia y los pocos beneficios económicos que se obtienen al llevar adelante casos de manera individual".[267] A nivel mundial, hubo un incremento en la legislación de protección de datos, pero la aplicación adecuada sigue siendo un desafío.[268]

Una de los cinco tipos básicos de reparación ante las vulneraciones de derechos humanos es la restitución o restauración, es decir, el restablecimiento del individuo a la misma situación en la que

260. Ver, p. ej. Kang y Vogel, *Tech giants amass a lobbying army, NYT and Fang, Silicon Valley-funded privacy think tanks fight in DC,* The Intercept, abril 2019

261. Para la Ley de confidencialidad del consumidor de California, ver, p. ej. Kartikay Mehrotra, Laura Mahoney y Daniel Stoller, *Google and other tech firms seek to weaken landmark California data-privacy law*, Los Angeles Times, 4 de septiembre de 2019, https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law. Para la Ley de confidencialidad de datos biométricos de Illinois, ver, p. ej. Russell Brandom, *Facebook-backed lawmakers are pushing to gut privacy law*, The Verge, 10 abril de 2018, https://www.theverge.com/2018/4/10/17218756/facebook-biometric-privacy-lobbying-bipa-illinois

262. Carole Cadwalladr y Duncan Campbell, *Revealed: Facebook's global lobbying against data privacy laws,* The Guardian, 2 de marzo de 2019, https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment

263. Google, *Our Principles and Standards of Business Conduct,* https://www.google.com/publicpolicy/transparency/, y *Trade Associations and Membership groups,* https://services.google.com/fh/files/misc/trade_association_and_third_party_groups.pdf

264. Respuesta de Facebook, ver el anexo que se incluye.

265. El derecho a una reparación efectiva ha sido reconocido en distintos instrumentos y tratados regionales e internacionales de derechos humanos, y también como una norma de derecho consuetudinario internacional. Ver, p. ej., artículo 8, Declaración Universal de los Derechos Humanos; artículo 2 (3), Pacto Internacional de Derechos Civiles y Políticos; artículo 2, Pacto Internacional de Derechos Económicos, Sociales y Culturales.

266. Ver, por ejemplo, Reuters, *European regulators: We're not ready for new privacy law,* mayo de 2018, https://uk.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUKKBN1I915X; Agencia de los Derechos Fundamentales de la Unión Europea (FRA), *Access to data protection remedies in EU Member States*, 2013, p. 46, https://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

267. Noyb, *Making Privacy a Reality*, 2017, p. 8, https://noyb.eu/wp-content/uploads/2017/11/concept_noyb_public.pdf

268. Consumers International, *The state of data protection rules around the world*, mayo de 2018, p. 5 https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf; Privacy International, *The Keys to Data Protection*, agosto de 2018, p. 7, https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

se encontraba antes de la violación de sus derechos. Sin embargo, en el contexto de la extracción de datos de forma masiva y la vigilancia corporativa, la restitución puede ser casi imposible. El ACNUDH explica con claridad que "las consecuencias de ese tipo de abusos son difíciles de reparar... La facilidad para conservar, intercambiar, reutilizar y fusionar datos y perfiles influye en la perdurabilidad de los datos digitales, lo que significa que las personas pueden enfrentarse a riesgos nuevos o persistentes para sus derechos en el futuro".[269]

El acceso a información sobre cómo impactan las operaciones de una empresa en sus derechos es esencial para que las personas puedan hacer valer su derecho a una reparación efectiva en casos de abusos de derechos humanos por parte de las empresas.[270] No obstante, la asimetría de información entre Google y Facebook y los usuarios de Internet y la complejidad de los procesos relacionados con la forma en que los datos se recopilan, procesan y comparten implica que las personas a menudo no pueden siquiera encontrar información que indique si sus derechos se vieron afectados o no y de qué manera.[271] Tomemos como ejemplo el caso de los datos de Facebook que recolectó Cambridge Analytica. El académico David Carroll ha pasado dos años intentando recuperar sus datos de Cambridge Analytica, pero todavía no pudo lograrlo. Si el incidente no hubiera salido a la luz gracias al trabajo de los periodistas de investigación, Carroll ni siquiera sabría que sus datos se usaron de manera indebida.[272]

El Relator Especial de las Naciones Unidas sobre la libertad de expresión destacó la forma en que los sistemas de inteligencia artificial, en general, suelen interferir con el derecho a una reparación efectiva.[273] Hay un desafío inherente al proceso de informar, ya que "las personas no están al tanto del alcance, la magnitud o incluso la existencia de sistemas algorítmicos que afectan sus derechos". Esa falta de transparencia se exacerba porque los algoritmos de las empresas se adaptan y cambian constantemente. En consecuencia, hasta los diseñadores del sistema podrían tener dificultades para explicar cómo llegaron a los resultados.[274]

Finalmente, la naturaleza inherentemente colectiva de los impactos algorítmicos en la magnitud de los sistemas de Facebook y Google plantea desafíos a la hora de obtener una reparación a nivel individual. Los sistemas de reparación a menudo no están diseñados para manejar impactos a una escala tan grande e imprecisa.[275] Como destacan Lilian Edwards y Michael Veale, expertos en derechos digitales y tecnología, "la reparación en los casos de protección de datos se basa esencialmente en derechos individuales… mientras que las vulneraciones derivadas de los algoritmos suelen surgir de la estigmatización o la clasificación en grupos que realizan los algoritmos".[276]

269. ACNUDH, *El derecho a la privacidad en la era digital*, A/HRC/39/29, 2018, párrafo 56

270. Amnistía Internacional, *Injustice Incorporated: Corporate Human Rights Abuses and the Right to Remedy,* 2014, p. 157

271. The Human Rights, Big Data and Technology Project, Universidad de Essex, presentación ante el ACNUDH sobre El derecho a la privacidad en la era digital, 2018, p. 8

272. Wired, One Man's Obsessive Fight to Reclaim His Cambridge Analytica Data, enero de 2019, https://www.wired.com/story/one-mans-obsessive-fight-to-reclaim-his-cambridge-analytica-data/

273. David Kaye, 2018, párrafo 40

274. AI Now Institute, *Annual Report*, 2017, p. 30 https://ainowinstitute.org/AI_Now_2017_Report.pdf

275. Berkman Klein Center for Internet & Society, *Artificial Intelligence & Human Rights: Opportunities & Risks*, p. 55 https://cyber.harvard.edu/sites/default/files/2018-09/2018-09_AIHumanRightsSmall.pdf?subscribe=Download+the+Report

276. Edwards y Veale, 2017, p. 22

CONCLUSIÓN Y RECOMENDACIONES

El advenimiento del modelo de negocios basado en la vigilancia llevó a que dos empresas —Google y Facebook— controlen una arquitectura de vigilancia que no tiene parangón en la historia de la humanidad. El sistema abarca continentes completos y afecta al menos a un tercio de la población mundial. En su forma actual, el modelo de negocios basado en la vigilancia es incompatible con el derecho a la privacidad y representa una amenaza grave para otro conjunto de derechos humanos.

En la práctica, los problemas detallados en este documento exceden a Google y Facebook. El modelo de negocios basado en la vigilancia no solo es funcional a los intereses de esas empresas hegemónicas. Se ha convertido en el núcleo de muchas empresas: desde anunciantes hasta agentes de datos, empresas emergentes y compañías fuera del sector de la tecnología que quieren crecer o cambiar el rumbo de sus negocios para monetizar los datos personales. El modelo que introdujeron Google y Facebook se convirtió en el prototipo de Internet y está llegando a los hogares, los lugares de trabajo y la calle por medio de la "Internet de las cosas".

Y, sin embargo, a pesar de lo que se ha hecho creer a las personas de todo el mundo que usan estas plataformas, no es *necesario* que Internet dependa de la vigilancia. Los graves abusos a la privacidad, la libertad de expresión y otros derechos humanos no son inherentes a la tecnología detrás de Internet, sino al modelo de negocios que se ha convertido en el modelo dominante. Facebook y Google eligieron su modelo de negocios precisamente porque era la forma más rápida de hacer que sus empresas crecieran. Ahora está claro que su elección tiene consecuencias profundas y de gran alcance respecto de los derechos humanos.

La escala y la complejidad de las vulneraciones de derechos humanos vinculadas con los negocios basados en la vigilancia requerirán una "combinación innovadora" de soluciones estructurales. Será necesario llevar a cabo investigaciones, análisis y reflexiones interdisciplinarias de forma permanente con una amplia variedad de participantes —tecnólogos, académicos, la sociedad civil, expertos en políticas y líderes políticos— para encontrar un conjunto de soluciones adecuado. En la actualidad, ya existe un corpus considerable de investigación académica y una comunidad multidisciplinaria está trabajando activamente en estas cuestiones.

Los riesgos para la privacidad que representa este modelo de negocios se vienen registrando desde hace tiempo. Hace 20 años, cuando se estaban implementando las bases del sistema, los defensores de la privacidad alertaron sobre los peligros de la elaboración individualizada de perfiles en línea y destacaron la necesidad de medidas legales de protección. En el año 2000, Marc Rotenburg, director de Electronic Privacy Information Center, le dijo al Senado de Estados Unidos: "Les advertimos [hace un año] que la autorregulación no lograría proteger la privacidad y que habría un rechazo público en contra del plan de la empresa para elaborar perfiles de los usuarios de Internet".[277]

277. Marc Rotenburg, *On Internet Privacy and Profiling*, testimonio frente al Comité de Comercio del Senado de Estados Unidos, junio del año 2000, https://epic.org/privacy/internet/senate-testimony.html. La empresa a la que se hizo referencia era DoubleClick, una empresa de anuncios de tecnología, que posteriormente adquirió Google.

Sin embargo, ahora surgió una gran oportunidad para abordar el problema de una vez por todas. De la opinión pública predominante sobre el poder de las grandes empresas de tecnología en los mercados más grandes se desprende claramente que pronto se aplicarán más regulaciones gubernamentales en el sector. El riesgo está en que toda regulación sobre Internet debe implementarse con mucho cuidado para no perjudicar la libertad de expresión ni otros derechos. Por lo tanto, es esencial que, independientemente de la forma que adopte, el nuevo sistema regulatorio se base en un enfoque centrado en los derechos humanos y aborde el impacto inherente del modelo de negocios basado en la vigilancia respecto del derecho a la privacidad y otros derechos humanos. En el corto plazo, hay una necesidad imperativa de fortalecer la aplicación de la regulación existente frente a las vulneraciones generalizadas y sistémicas de las leyes de protección de datos.

Los estándares y las leyes de derechos humanos ya establecen con claridad que los Estados tienen la obligación y los actores privados tienen la responsabilidad de tomar medidas inmediatas y efectivas para proteger y respetar (según corresponda) el derecho a la privacidad. En 2016, el Consejo de Derechos Humanos detalló un conjunto de medidas que deberían adoptar los Estados para promover y proteger los derechos humanos y las libertades fundamentales en Internet e instó a los Estados a "adoptar, aplicar y, de ser necesario, reformar leyes, reglamentos, políticas y medidas relativas a la protección en línea de los datos personales y la privacidad".[278]

No es posible abordar esta cuestión desde un único enfoque. Las iniciativas para establecer límites más estrictos en cuanto al rastreo y al uso de datos personales no serán suficientes si no se aborda también la concentración de datos —y de poder— en las manos de Facebook y Google. A su vez, el creciente grupo de políticos, autoridades reguladoras e intelectuales que proponen que se "dividan" las grandes empresas de tecnología no logrará abordar la cuestión de los abusos sistémicos de derechos humanos a menos que exija medidas que enfrenten de manera holística el modelo de negocios basado en la vigilancia.

El objetivo de este informe es introducir una perspectiva de derechos humanos en la discusión y proponer una posible solución.

RECOMENDACIONES PARA LOS ESTADOS

- Los Estados deben tomar medidas para garantizar que el acceso a infraestructuras y servicios digitales y el uso de estos —incluidos los que proporcionan Google y Facebook— no dependan de la vigilancia permanente. Para eso, será necesario promulgar y aplicar leyes que garanticen a las personas el derecho de "no someterse al seguimiento" realizado por anunciantes y otros terceros.
- El primer paso es evitar que las empresas condicionen el acceso a sus servicios a la obtención del "consentimiento" de los usuarios para que se recopile, procese o comparta su información personal con fines de marketing o publicidad.
- Los Estados deben promulgar y aplicar leyes de protección de datos ejemplares en las que los derechos humanos ocupen un lugar central y que estén en línea con los principios de protección de datos establecidos. Esas leyes deben restringir la cantidad y el alcance de los datos personales que se pueden recopilar, limitar de manera estricta la finalidad con la cual las empresas procesan esos datos y garantizar la protección de las inferencias acerca de las personas que se obtienen de la recopilación y el procesamiento de los datos personales. Asimismo, deberían exigir que las empresas les comuniquen a los usuarios de manera clara la finalidad con la cual recopilan sus datos personales desde un principio y que no los procesen de una forma que sea incompatible con esa finalidad o con su responsabilidad en relación con los derechos humanos.
- Los Estados también deben garantizar que las autoridades nacionales de protección de datos sean realmente independientes y tengan la experiencia y los recursos adecuados para investigar a fondo y sancionar las infracciones por parte de Google, Facebook y otras grandes empresas

278. Consejo de Derechos Humanos de la ONU, Promoción, protección y disfrute de los derechos humanos en Internet, junio de 2016, documento A/HRC/32/L.20

de tecnología. Además, deben garantizar que existan mecanismos de reparación efectivos, tanto individuales como colectivos.

- Los Estados deben implementar regulaciones, desarrolladas con el asesoramiento de grupos afectados y expertos técnicos independientes, para garantizar la supervisión del diseño, el desarrollo y la implementación de los sistemas algorítmicos a fin de asegurar que las empresas sean legalmente responsables de las vulneraciones de derechos humanos vinculadas con dichos sistemas, incluidos los impactos negativos que surjan de las decisiones de optimización de dichos sistemas. Eso es particularmente importante para sistemas con la escala y el impacto de las plataformas de Google y Facebook.
- Los Estados deberían exigir legalmente que las empresas de tecnología lleven a cabo procesos de diligencia debida de derechos humanos para identificar y abordar el impacto de sus operaciones globales respecto de los derechos humanos, incluidos los riesgos y abusos vinculados a sus sistemas algorítmicos o que surjan de su modelo de negocios en general.
- Los Estados deben adoptar políticas públicas relacionadas con Internet que se centren en el acceso y disfrute universal de los derechos humanos. Eso incluye medidas disruptivas para el mercado y para los incentivos a los modelos de negocios basados en la vigilancia corporativa.
- Los Estados deben promulgar o aplicar marcos regulatorios para garantizar que las personas puedan ejercer en la práctica el derecho a elegir alternativas que respeten la privacidad en lugar de modelos basados en la vigilancia. Eso incluye medidas que garanticen la interoperabilidad en lugar de la simple portabilidad de datos para que las personas puedan pasar de un servicio a otro sin perjuicio social y para mitigar el efecto de red.
- Los Estados deben garantizar el acceso a una reparación efectiva para las vulneraciones de derechos humanos vinculadas a los impactos de las empresas de tecnología, independientemente de dónde ocurran las vulneraciones e incluidas aquellas vulneraciones que deriven de operaciones llevadas a cabo por sus subsidiarias (extranjeras o locales).
- Los Estados deben invertir en la implementación de programas de educación digital efectivos y promoverlos para garantizar que las personas conozcan sus derechos, incluido el derecho de acceder a una reparación ante los abusos de protección de datos, de privacidad y de otros derechos humanos que se produzcan al acceder a servicios digitales.

RECOMENDACIONES PARA LAS EMPRESAS

- Google, Facebook y otras empresas de tecnología que dependen de operaciones invasivas basadas en datos que constituyen instancias de vigilancia corporativa masiva deben encontrar la forma de pasar a un modelo de negocios que respete los derechos. Como primer paso, las empresas deben garantizar que las políticas y los procesos de diligencia debida de derechos humanos aborden el impacto sistémico y generalizado de su modelo de negocios respecto de los derechos humanos, en especial respecto del derecho a la privacidad, y deben comunicar con transparencia cómo identifican y abordan esos impactos y todo riesgo para los derechos humanos o abuso de derechos humanos.
- Las empresas de tecnología deben evitar hacer lobby para lograr la laxitud de la legislación y las políticas de privacidad y protección de datos si dicha laxitud aumenta el riesgo de abusos de derechos humanos. En sus esfuerzos para respetar los derechos humanos, las empresas no deben perjudicar la capacidad de los Estados de cumplir con sus propias obligaciones de derechos humanos.
- Las empresas de tecnología deben tomar medidas para reparar todo abuso de derechos humanos al que hayan contribuido o que hayan causado a raíz de sus operaciones empresariales.

Anexo: Carta de Facebook - Página 1

Dear Tanya and Joe,

Thank you for the opportunity to respond to the summary of your forthcoming report about human rights and Facebook's business model. While we appreciate the opportunity to engage with Amnesty International on these important issues, we respectfully disagree with your conclusion that our practices are inconsistent with human rights principles.

Like many other online companies, Facebook is supported through the sale of advertising. This enables billions of people around the world to connect and express themselves, on an unprecedented scale. Amnesty International itself has benefited from this ability to connect: The organization has relied on Facebook ads and other Facebook products to reach supporters, raise money, and advance your mission.

Our business model is what allows us to offer an important service where people can exercise foundational human rights—to have a voice (freedom of expression) and be able to connect (freedom of association and assembly). That's why we were disappointed to see that Facebook's clear contributions to human rights (and human rights organizations) are not mentioned in the "summary of analysis" you shared with us. There are countless examples of how people have used Facebook to advance human rights around the world. And, as a company, we're committed to respecting human rights, including the right to privacy. Our longstanding membership in the Global Network Initiative (GNI)—and our adherence to the governance, privacy, and freedom of expression standards enshrined in the GNI Principles and Implementation Guidelines—reflect this commitment. As you know, these standards are grounded in the UN Guiding Principles for Business and Human Rights (UNGP), the Universal Declaration of Human Rights (UDHR), and the International Covenant on Civil and Political Rights (ICCPR). We are independently assessed every two years on our implementation of our obligations as a GNI member company.

This is an important moment for human rights at Facebook. We recently updated our staffing and leadership on human rights issues, and have just issued new Community Standards Values that explicitly refer to human rights principles. We're engaged in multiple, major, human rights impact assessments, and are about to launch one of this decade's most exciting rights-related experiments, Facebook's Oversight Board. Accompanied by the recent explicit commitment of our top leadership to freedom of expression, and in the midst of designing a significant new initiative for human rights defenders, you can be confident there is much more rights-related work to come.

It also an important moment for privacy at our company. Our robust privacy review process, which brings together a cross-company group of experts to review new products and privacy-related changes to existing products, is about to become even stronger as we implement our recent settlement with the Federal Trade Commission.The settlement requires an unprecedented level of accountability, imposing controls that have never before been required of a company in our industry.

We appreciate the opportunity to respond to the summary you sent us, but we are deeply concerned that it contains a number of inaccuracies and faulty assumptions, the most serious of which we outline here:

1. **Facebook's Business Model and "Surveillance."** Describing Facebook's business model -- which involves selling ads in order to offer services for free -- as "surveillance-based" elides the crucial difference between services that people voluntarily sign up to use, and the involuntary government surveillance that defines the arbitrary interference with privacy, home, family, or correspondence envisaged under article 17 of the International Covenant on Civil and Political Rights.

2. **Data Collection.** We do not "collect as much data about people as possible" or infer people's sexual identity, personality traits or sexual orientation. In fact, we only require

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

people to provide their name, age, gender, and contact information when they sign up for Facebook. We do not have access to the contents of anyone's email.

3. **Non-users.** Like other companies that provide technologies to other websites and apps, we may receive information about non-users when they use those websites and apps. This is part of the basic function of the Internet. We do not use non-user information to build profiles about people.

4. **Interoperability.** Part of our vision for enabling people to message across our apps is making those messages end-to-end encrypted. This means we will collect **less** data about people -- not more, as the summary suggests.

5. **Social plugins.** We do not store data from social plugins (such as the Like button) in identified form unless that's necessary for safety, fraud prevention or security.

6. **Free Basics.** The purpose of Free Basics was not to "gain access to new sources of data." Free Basics does not store information about the things people do or the content they view within any third-party service available through Free Basics.

7. **Engagement.** Our News Feed algorithm is not designed to "maximise engagement." The goal of News Feed is to connect people with the content that is most interesting and relevant to them. Our focus is on the quality of time spent on Facebook, not the amount.

8. **Discrimination and transparency.** The summary fails to mention the many changes we have made to our ads systems in order to help prevent discrimination -- measures that remain unmatched in the industry. Facebook is far from the only place where advertisers run ads for opportunities like housing, employment and credit and we've made fundamental changes for how these ads run on our services. Many of the interest segments mentioned in the summary have also been removed. Transparency is a significant part of how we're addressing this issue, and we have made it easier to see all the ads running on Facebook, regardless of whether they are shown to you.

9. **App Developers.** The summary similarly fails to mention the work we have done to limit the misuse of people's information that we saw in the Cambridge Analytica matter. The summary's suggestion that we recently suspended 10,000 developers because of suspected data misuse is flatly incorrect.

10. **Law enforcement.** Far from "contributing" to unlawful government surveillance, we actively push back against it, scrutinizing every request we receive to ensure it complies with accordance with our terms of service, applicable law, and international human rights standards.

You will note that our processes far exceed the minimum standards set out in the UN's latest guidance on this issue, *The Right to Privacy in the Digital Age.* We hope these points -- and the additional context below -- will help you revise your arguments on surveillance, privacy, and proportionality as you finish your report.

We fully recognize that Facebook has made mistakes in the past, and are committed to continually improving our services and incorporating feedback from the people who use them. We would welcome the opportunity to engage further with you on your report and the important issues it raises.

Sincerely,

Steve Satterfield

Director, Privacy & Public Policy

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

Facebook's Business Model and Data Practices

Your summary characterizes Facebook's business model as "surveillance-based." We strongly disagree with this suggestion.

First, it is important to note that **no one is obliged to sign up for Facebook.** The decision to use our family of apps is entirely voluntary and personal. A person's choice to use Facebook's services, and the way we collect, receive or use data -- all clearly disclosed and acknowledged by users -- cannot meaningfully be likened to the involuntary (and often unlawful) government surveillance and interception of communications defining the kind of arbitrary interference with home, correspondence, or family life envisaged under article 17 of the International Covenant on Civil and Political Rights.

Second, Facebook's business model is not, as your summary suggests, driven by the collection of data about people. Like many other online companies, Facebook is supported through the sale of advertising. As you correctly note, we do not sell data; we sell ads. Doing so allows us to **offer a service that enables everyone to exercise foundational human rights—to have a voice (freedom of expression) and be able to connect (freedom of association and assembly).**

While using the data we collect and receive is an important part of showing effective ads, it is incorrect to suggest that our business model is driven by the desire to collect "as much data about people as possible." Data collection is not an end in itself for Facebook, but rather is the way we provide relevant and useful services to people and organizations. **The only data we require people to provide when signing up for Facebook are the person's name, age, gender, and contact information.** We also enable people to express their gender identity in ways that go beyond male and female.

Over time, as people use our products, we may receive additional data (e.g., the Pages a person likes, the posts and ads they click on), and this data helps us provide content and services that are more relevant to them, such as determining which posts and ads appear higher up in their News Feeds.

Your summary misstates the nature of the data we collect and receive from people. **We do not read the content of people's emails, nor do we infer people's sexual identity, personality traits or sexual orientation. We also do not use the content of people's messages to other people for ad targeting.**

Third, it is vitally important to note the range of controls we give people over the data we collect, store and use. We provide strong controls to allow people to decide what is right for them. This is why we offer tools such as Access Your Information, Ad Preferences and "Why am I seeing this ad?", all of which we are constantly working to improve. We also recently started rolling out a new way for users to view and control off-Facebook activity, and to disconnect this information from their accounts. **These tools provide unprecedented levels of transparency and control,** and strongly surpass the minimums defined in paragraph 30 the UN's most recent thinking on this topic, The Right to Privacy in the Digital Age. Our steady introduction of privacy-protected tools like these belies the summary's suggestion that "Facebook can afford to abuse privacy." To the contrary, we know that if we do not protect people's data, we will lose their trust.

As noted above, data allows us to make ads more relevant. Not only is this a better experience for people; it also has been crucial for the millions of small businesses who have access to the same powerful tools that large businesses do, allowing them to reach people who are more likely to be interested in their products, services, or causes. The efficiency that data brings to advertising has helped businesses and other organizations around the world to grow and advance important

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

causes, including freedom of assembly and association; rights to freedom of expression and political participation; and of course, the right to development.

The summary's suggestion that our goal of making our services more interoperable will enable us to aggregate *more* data about people is flatly incorrect. As our CEO Mark Zuckerberg explained, our vision for the future operation of our services involves making them end-to-end encrypted — which means we will receive ***less* data about people, not more.** End-to-end encryption means that we'll be unable to access the content of people's messages for advertising—or for any other reason.

It is also worth noting that, other than for security purposes and guarding against fraud, **Facebook no longer stores data from social plugins (such as the Like Button) with user or device identifiers.** The limited data that we do keep for security and fraud investigations is stored in separate, access-controlled tables to help ensure that only the relevant security or integrity employees have access to that information. Once the investigation concludes, the data is deleted unless we determine abusive activity has occurred and further action is necessary to protect our products and users.

Although it is correct that we may receive information about people without Facebook accounts when they use a website or app that includes a social plugin (or other Facebook technology), **we do not build profiles about non-users.**

The report's characterization of our Free Basics service is inaccurate. **The Free Basics privacy statement makes clear that the service is not a "data extraction exercise."** To the contrary, Free Basics safeguards people's privacy through strong protections. **Most importantly, Free Basics does not store information about the things people do or the content they view within any third-party service**. Rather, in order to provide access to those services free of data charges, Free Basics temporarily stores only the domains or names of the third-party services visited, after which this information is aggregated or otherwise de-identified. Free Basics continues to be an important tool for bringing more people online and providing a baseline of connectivity for people around the world.

Improving People's Experiences in News Feed

Amnesty's executive summary incorrectly suggests that our algorithms are designed to promote sensationalist content because people are more likely to engage with that content. **The actual goal of Facebook's News Feed is to connect people with the content that is most interesting and relevant to them. Our focus is on the quality of time spent on Facebook,** not the amount. Because the space in each user's News Feed is limited, Facebook's algorithms prioritize posts that are predicted to spark meaningful conversations — including posts from close friends, family, and pages users interact with frequently. This type of content is prioritized over public content, including posts from businesses, brands, and media.

We have also taken steps to reduce the incidence of content that may be engineered to game engagement on Facebook, but that results in a negative or harmful experience for users. For example, we've introduced systems to detect and reduce the distribution of content such as engagement bait, hoaxes, fake news, and clickbait. And we have worked very hard, and successfully, to reduce the virality of hate speech and other inflammatory content in many countries at risk of violence.

We also believe in giving users more information about and control over what they see on Facebook, including on News Feed. In March 2019, we announced a new transparency initiative called "Why I am seeing this post?" which gives users access, for the first time ever, to ranking information about each post in their Feed. We also have tools that allow users to further

personalize how they experience News Feed, such as viewing posts in chronological order or choosing to see posts from a particular Page of person at the top of Feed.

Taking Action to Prevent Discrimination and Improve Transparency

One of our top priorities is protecting people from discrimination on Facebook. Our advertising policies have long prohibited discrimination, and we require all advertisers globally to certify compliance with our non-discrimination policy in order to run ads on Facebook.

We are now making fundamental changes in how U.S. housing, employment and credit opportunity ads can run on Facebook. We will not allow advertisers to target these ads to people based on age, gender, ZIP code or any interests describing or appearing to relate to protected characteristics. These changes will be fully implemented by the end of 2019; they're the result of settlement agreements with leading civil rights organizations and ongoing input from civil rights experts. This settlement also included a **commitment that we work with the civil rights community and other experts to study the potential for bias in connection with the algorithms we (and others in the industry) use to show people relevant content and ad**s.

Even before the settlement, we had made changes to the ads system, which advertisers use to select the audience for their ads. We removed thousands of categories from that could potentially relate to protected characteristics. Our review of these audience selection options is continuous and informed by feedback from outside experts.

We are also **building a new section of our Ad Library** that will give people the ability to search for and view all current housing ads in the U.S. by location chosen by the advertiser, regardless of whether a person is in the intended audience. We'll introduce similar sections for U.S. employment and credit ads next year.

These transparency efforts build on our efforts referenced in the report to bring greater transparency to political and issue ads on Facebook. Among other things, these efforts are intended to address so-called "dark ads" that you refer to. We continue to work on more ways to provide transparency in this space, and we appreciate the feedback we have received from the organizations cited in your report.

Addressing Potential Misuse of Facebook Platform Data by Third-Party App Developers

The Cambridge Analytica matter involved a third-party app developer — Aleksandr Kogan — who violated Facebook's policies by selling users' information to a third party, Cambridge Analytica. When we became aware of this issue, we took action quickly to investigate, and we secured sworn certifications from Kogan, Cambridge and others that they had deleted the relevant data. In 2018, reports surfaced that Cambridge may have not, in fact, deleted the data it received from Kogan.

We recognize that Cambridge involved a breach of trust, and we have taken a number of steps to help prevent something like it from happening again. These steps include:

- Reducing the kinds of data that people may share with app developers;
- Preventing apps that a person has not used for more than 90 days from continuing to access a person's data through Facebook;
- Strengthening our App Review process by requiring more apps to submit to upfront review before being able to ask people to share their data;
- Conducting an investigation of apps that had access to large amounts of user information before we changed our Platform in 2015 to prevent people from sharing their friends' information with apps; and

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

- Suspending — and even suing — developers who fail to cooperate with this investigation.

With respect to this investigation, your report states "ten thousand . . . apps were suspended for potentially misusing data." This is incorrect. As we explained in our most recent update on this investigation (which thus far has addressed millions of apps), we have suspended tens of thousands from around 400 developers. Suspension is not necessarily an indication that these apps were posing a threat to people. Many apps were not live but were still in their testing phase when we suspended them. It is not unusual for developers to have multiple test apps that never get rolled out. And in many cases, the developers did not respond to our request for information so we suspended them.

You are correct that carrying out an investigation of this kind is difficult, but it is not accurate to suggest that we do not have sufficient tools at our disposal to identify and take action against developers we have found to have violated our policies. **We are committed to taking strong action — including by taking developers to court, as we have done recently.**

Finally, our new agreement with the FTC also will bring its own set of requirements for oversight of app developers on our Platform. It will require developers to annually certify compliance with our policies. Any developer that fails to follow these requirements will be held accountable.

Protecting Privacy In Connection with Requests from Law Enforcement

Facebook discloses account records in response to valid legal requests in accordance with our terms of service, applicable law, and international human rights standards. Because we are deeply concerned about protecting our users' data, **we carefully scrutinize every request to ensure it meets those requirements.** When we don't believe those standards have been met, we decline to provide the requested data and, if necessary, challenge the request in court. We've done this, for example, when the requesting government exceeded its authorities in making the data request, or we are concerned the request doesn't comply with international human rights standards.

We openly publish how we enforce our Community Standards, and how we respond to government data requests, in our regular Transparency Reports. They are worth studying.

Engaging With Government Officials on Important Public Policy Issues

As we've said in our annual political engagement statement, public policy decisions can have significant implications for the people who use our services and the future direction of our company. Facebook regularly engages with government officials to discuss a range of policy issues as well as share information about our products and services. In doing so, we maintain compliance with all relevant laws and guidelines. All Facebook Personnel, including external consultants, who engage with government officials to discuss policy issues on our behalf receive training on the ethical standards required in all such interactions.

facebook

Address: 1 Hacker Way
Menlo Park, CA 94025

AMNISTÍA INTERNACIONAL ES UN MOVIMIENTO GLOBAL POR LOS DERECHOS HUMANOS. CUANDO UNA PERSONA ES VÍCTIMA DE LA INJUSTICIA, NOS AFECTA A TODOS.

CONTÁCTANOS

info@amnesty.org

+44 (0)20 7413 5500

PARTICIPA EN EL DEBATE

www.facebook.com/AmnestyGlobal

@AmnestyOnline

GIGANTES DE LA VIGILANCIA:

LA AMENAZA QUE EL MODELO DE NEGOCIOS DE GOOGLE Y FACEBOOK REPRESENTA PARA LOS DERECHOS HUMANOS

Google y Facebook ayudan a conectar el mundo y brindan servicios cruciales a miles de millones de personas. Para tener una participación significativa en la sociedad y la economía actual, las personas dependen tanto del acceso a Internet como de las herramientas que Google y Facebook ofrecen.

Pero, más allá del valor real de sus servicios, las plataformas de Google y Facebook implican un costo sistémico. Para disfrutar de sus derechos en línea, las personas se ven obligadas a aceptar un monitoreo constante en Internet y en el mundo físico, por ejemplo, mediante dispositivos conectados. El modelo basado en la vigilancia de Facebook y Google es inherentemente incompatible con el derecho a la privacidad y representa una amenaza para otros derechos más, incluidos la libertad de opinión y de expresión, la libertad de pensamiento y el derecho a la igualdad y a la no discriminación.

Los gobiernos deben tomar medidas positivas para reducir los daños que genera el modelo de negocios basado en la vigilancia, como adoptar políticas públicas que tengan como objetivo garantizar el acceso universal y el pleno ejercicio de los derechos humanos; reducir o eliminar la continua vigilancia de entidades privadas; e implementar reformas estructurales que resulten suficientes para reinstaurar la confianza en la Internet. Google, Facebook y otras empresas de tecnología deben terminar con la vigilancia omnipresente y pasar a un modelo de negocios que respete los derechos.

Índice: POL 30/1404/2019
Noviembre de 2019
amnesty.org

AMNESTY INTERNATIONAL