IX
Dar aceptar: Google, Facebook y WhatsApp se apropian de nuestros datos

"Durante décadas, las computadoras nos ayudaron a recordar,
pero ahora es tiempo de que nos ayuden a ignorar."

Cory Doctorow

"El monitoreo total es inevitable.
Esconderlo, mentir sobre él, no lo es."

Kevin Kelly

Cuando cumplí cinco años en mi trabajo mi jefe me regaló un reloj inteligente. El pequeño aparato, de tres centímetros por cuatro, 150 gramos de peso con caja incluida, estaba fabricado para adaptarse a mi vida. Con una batería diseñada para durar siete días, capacidad para sumergirse 50 metros en agua, recibir mensajes, llamados y escuchar mi música preferida, era el compañero perfecto para el exilio en una isla desierta.

Mi jefe, un ingeniero genuinamente apasionado por la tecnología, pensó que el reloj era el mejor regalo para experimentar lo que el marketing llama la "vida *smart*": objetos que se adaptan al ambiente y a nuestras costumbres, a cambio de que les demos información para que eso suceda.

"Encuéntrate con Pebble, el reloj inteligente que se vuelve más in-

teligente con las nuevas aplicaciones creadas diariamente", decía la caja de diseño minimalista, blanca, el mismo color del *gadget*. Detrás de un envoltorio transparente, sus especificaciones de fábrica me aseguraban que, si lo extraía de ese cofre de cartón y decidía atarlo a mi muñeca, podía mantenerme conectada al mundo durante una semana prescindiendo de la electricidad. Me permitía, incluso, personalizar la pantalla con la cara de mi mascota.

Pero nunca me gustaron las mascotas. La idea de un animal que depende de que lo alimente a cambio de vivir encerrado en la ciudad siempre me pareció triste. El reloj era como un animal. Sólo que en vez de comida y un pote de agua diario, me pedía algo —tal vez menos tangible pero más valioso— para convertirse en mi compañero de vida más eficiente: todos los datos de mis llamadas, contactos, mails, preferencias musicales, imágenes, mis interacciones en las redes sociales. Y me prometía que, en el futuro, a medida que fuera sumando nuevas aplicaciones para hacerme la vida más eficiente, también me pediría otros detalles personales: mi pulso, el recorrido de mis caminatas diarias a través del GPS, las calorías que consumía diariamente y otros datos de mi cuerpo.

Extraer el reloj de la caja, pensé, implicaba un costo muy alto. No sólo suponía sacrificar mi naturaleza ajena a la dependencia, sino que significaba darle a ese pequeño aparato toda mi información personal (para que siempre pudiera ubicarme, comunicarme, ofrecerme el producto o servicio exacto que necesitara). Era entregarle a ese fragmento de plástico, zinc y titanio cada huella de mi vida digital. Pero el trato no era sólo con un objeto. Al firmar el contrato, a través de sus términos y condiciones, también lo hacía con la empresa que lo había fabricado, con los desarrolladores del programa que ahora gestionaría mis datos, y con quienes se proponían administrar esa información que yo dejaría en las aplicaciones y servicios. Les daba, para que dispusieran de ella, mi presencia permanente, mi comunicación sin cortes, para que siempre pudieran encontrarme y saber de mí. Con eso, también les decía con quién y dónde estaba, con quién hablaba, a quién le decía "te amo".

En 1962, en su "Preámbulo a las instrucciones para dar cuerda al

reloj"[186], Julio Cortázar escribía que cuando te regalan un reloj no te ofrecen "solamente ese menudo picapedrero que te atarás a la muñeca y pasearás contigo". Te regalan, decía, "un nuevo pedazo frágil y precario de ti mismo, algo que es tuyo pero no es tu cuerpo, que hay que atar a tu cuerpo con su correa como un bracito desesperado colgándose de tu muñeca. Te regalan la necesidad de darle cuerda todos los días, la obligación de darle cuerda para que siga siendo un reloj; te regalan la obsesión de atender a la hora exacta en las vitrinas de las joyerías, en el anuncio por la radio, en el servicio telefónico. Te regalan el miedo de perderlo, de que te lo roben, de que se te caiga al suelo y se rompa. Te regalan su marca, y la seguridad de que es una marca mejor que las otras, te regalan la tendencia de comparar tu reloj con los demás relojes. No te regalan un reloj, tú eres el regalado, a ti te ofrecen para el cumpleaños del reloj".

Hoy, a más de cincuenta años de la publicación de ese cuento, el poder de los objetos y la tecnología sobre nuestras vidas sigue siendo el mismo. O peor. Ya no le damos cuerda a un reloj, pero mantenemos cargados y conectados toda clase de aparatos para confiarles a ellos y a los programas que los gobiernan nuestro tiempo, nuestras ansiedades, gustos, relaciones, consumos, búsquedas, problemas, alegrías y miedos. Todo en forma de datos. Datos de todo tipo, que pueden distinguirnos —o como se dice "construir nuestro perfil"— si los ponemos uno al lado del otro: sexo, edad, lugares que visitamos, cosas que nos gustan, gente con la que hablamos. Todos esos datos *somos* nosotros.

El aparato al que le cedemos esa información puede tener forma de reloj inteligente o de teléfono móvil o de computadora o de *smart TV*, o de cualquier cosa que se conecte a una red para intercambiar información. Nos gusta, además, coleccionar objetos, hacerlos interactuar entre sí. Si estamos lejos de uno siempre está el otro: dejamos el celular, pasamos a la tableta, prendemos la computadora. Al teléfono celular, incluso, le pedimos tanto que no lo concebimos lejos. Los llevamos a la cama, al baño, nos acompaña mientras trabajamos, o cuando vamos al cine, ce-

[186] En el libro *Historias de cronopios y de famas*.

namos, viajamos, estamos en la playa o en el aeropuerto. Ya no podemos estar sin él. Pero tampoco podemos *ser* sin él. Porque nos resuelve muchas cosas: es un teléfono, un reproductor de música, una cámara de fotos, un entrenador personal, una secretaria de citas, un buscador de noticias y restaurantes, una forma de encontrar amor, sexo, diversión, de mantenernos cerca de quienes queremos, o de husmear en las vidas de los que odiamos, de comentar en las redes sociales y de mostrar dónde estamos o queremos estar. Y en vez de vivir pendientes de darle cuerda para que nunca deje de funcionar ahora buscamos desesperados el enchufe o la batería, el wifi o el 4G. Cuando la electricidad falla o cuando la conexión desaparece, nos sentimos perdidos.

Como dice el antropólogo y escritor Néstor García Canclini, así como en su momento el reloj fue imprescindible y su falta generaba algunos miedos, ahora esos temores se trasladaron al teléfono móvil: tememos perderlo, que nos lo roben, que se rompa, perder la conexión. Y nos apuramos a cambiar el modelo o la marca cuando aparece en el mercado uno nuevo. "El reloj y el móvil requieren un gasto inicial, pero los móviles se diferencian porque sólo existen si seguimos invirtiendo", dice[187]. También señala la doble vida de una era donde nos suponemos libres, celebramos la movilidad permanente, el nomadismo trabajar en cualquier lugar gracias a la tecnología, pero donde "en verdad no todos pueden escapar a la exigencia de disponibilidad constante, la vigilancia de quienes te recuerdan que perteneces a una empresa y un lugar aunque estés en otra ciudad u otro país". En sus palabras: "Te regalan también la posibilidad de que el jefe te llame a las 11 de la noche y te encargue un trabajo de urgencia".

En un mundo de conexiones rápidas, donde estar siempre *online* es un deseo y a la vez una exigencia casi de *status*, la pregunta entonces es: "¿Dónde está el verdadero poder: en conectarse velozmente y con muchos, o en la posibilidad de desconectarse?".

Me respondo que, por ahora, prefiero poder desconectarme. Dejo

[187] García Canclini, Néstor. *Lectores, espectadores e internautas*, Barcelona, Gedisa, 2007.

entonces al reloj preso en su celda, su caja. La observo otra vez: si el reloj me hablara, su sonido sería un coro de sirenas, como las que tentaban a Ulises y sus navegantes y lo obligaban a amarrarse al mástil de su barco y a tapar con cera sus oídos para no sucumbir ante ellas.

La tecnología tiene un encanto similar. Nos propone vivir mejor, hacer todo más rápido, mantenernos al tanto de cada novedad, estar cerca de conocidos y desconocidos, divertirnos saltando de pantalla a pantalla. Pero, también, nos pide demasiado.

Un teléfono móvil o una computadora que nos resuelve ciertamente muchos aspectos de la vida también nos pide que le ofrendemos una parte de ella. Para que los aparatos, las aplicaciones y los programas funcionen, debemos abrirnos ante ellos, ceder nuestros datos e información personal. Desde que encendemos la computadora, dependiendo del sistema operativo que elijamos, cedemos a su fabricante y a sus programas asociados determinada información.

Cuando navegamos en internet, el buscador que utilizamos va monitoreando y guardando nuestras preferencias: desde lo que tipeamos, los avisos sobre los que hacemos clic, las páginas que visitamos, las aplicaciones que utilizamos, el lugar en donde estamos haciendo esa pesquisa. Cuando usamos nuestros celulares, las aplicaciones registran a través del GPS nuestra ubicación, nos piden acceder a los datos de nuestras llamadas, contactos, preferencias de búsquedas, compras, fotos, música. Cuando utilizamos redes sociales, cada paso que damos va dejando también nuestras preferencias: qué páginas nos gustan, qué comentarios y a qué fotos les damos "me gusta" (*like*), con qué marcas y personas interactuamos. Nuestras huellas digitales van quedando desperdigadas en el camino, pero muchas veces no somos conscientes de que las vamos dejando. Y otra veces, sabemos que eso sucede, pero preferimos no verlo. Entonces con un movimiento certero del mouse le damos *aceptar* a los términos y condiciones de todos los productos, servicios, aplicaciones y redes sociales sin leerlos. La tentación de llegar rápido a utilizarlos, a que nos resuelvan un problema, nos hagan algo más fácil, nos diviertan o nos permita encontrarnos con otros es más fuerte.

El problema es que los datos que vamos cediendo a nuestro paso no quedan dentro del objeto que estamos utilizando —un teléfono celular, una tableta, una computadora—. Tampoco se dispersan en el éter de la Red, ni en esa nube mágica donde las empresas nos hacen creer que se almacena la información. Cada rastro digital queda en manos de empresas, en sus granjas de servidores, compañías que construyeron esos objetos con programas y aplicaciones que recolectan esos datos. Nuestras huellas son el oro de esas corporaciones: miles de millones de elecciones de personas alrededor del mundo que les dan a las empresas una base de datos actualizada en tiempo real cada vez que nos tentamos con un "me gusta", cada vez que buscamos un producto para comprar o para saber qué piensan otros que lo adquirieron, cuando completamos un perfil con nuestras preferencias en una página o una aplicación de citas, cuando usamos una red social para opinar, chatear e interactuar con otros. A las empresas que inventaron esos programas —que no son más que conjuntos organizados de personas— no les importa lo que pensemos o cómo seamos: les importa lo que hacemos y lo que consumimos.

Los objetivos de recolectar nuestros datos *online* no son siempre los mismos, pero están relacionados. Algunos pueden querer tenerlos para dañarnos: robar una identidad, cometer todo tipo de delitos, entrar en nuestras cuentas, ver lo que hacemos por razones espurias. Otros lo hacen con intenciones de vigilancia y monitoreo: Estados de todos los países utilizan los pasos dados por millones de personas en la Red para conocer más de nosotros, para recopilar esa información y transformarla en un insumo de inteligencia con distintos fines. Y, también, están las empresas, a las cuales nuestros datos les interesan para construir perfiles cada vez más detallados de los consumidores, para ofrecernos lo que queremos comprar hoy o querremos tener mañana. Ese mercado de información personal es cada vez más grande, ayudado por todos los que, usando la Red, brindamos esa información, a veces siendo conscientes de los fines con los que será utilizada, y otras veces ignorándolo.

"El producto sos vos" es la frase más usada para explicar ese mecanismo por el cual internet evolucionó hasta convertirse en lo que es

hoy: una gran máquina de obtener y procesar datos a través servicios gratuitos para luego reutilizar toda esa información comercialmente. Si ayer buscamos en internet un pasaje a Nueva York, hoy nos ofrecerán el hotel. Pero aún más: si ayer nos interesó un pasaje y no lo compramos, hoy nos ofrecerán varias opciones más. Eso sí: serán probablemente más caros, porque el buscador habrá guardado una "*cookie*", un registro electrónico personalizado de nuestros caminos transitados por la Red que le dirá cuáles son nuestros intereses de consumo.

Si somos mujeres, jóvenes y a veces visitamos páginas de moda o belleza, nos tentarán con maquillajes o ropa. Pero si somos mujeres, jóvenes y visitamos blogs de autos, nos ofrecerán el modelo adecuado para nosotras. Si somos adolescentes, nos dirá qué película ver, qué concierto nos quiere allí. Y así para cada uno. Pero pueden ser también los sitios de noticias que visitamos y que "admiten cookies", capaces de seguir nuestro rastro de intereses: ¿nos gusta el deporte, el espectáculo, ambas cosas, o estamos interesados en la salud?

Pero además de usar la información para ofrecernos publicidad en forma directa, a través de avisos, los datos también se utilizan para hacer que los servicios que usamos en la Red nos ofrezcan "exactamente lo que queremos". Si dan con nuestro gusto, seguramente cliquearemos, es decir, compraremos. Un ejemplo es el cruce que realizan los buscadores (en nuestras computadoras o celulares) con la ubicación geolocalizada (a través del GPS, por ejemplo) que le ofrecemos voluntariamente. O con los los *check-ins* que realizamos en distintos lugares con aplicaciones como Foursquare o Swarm ("Ana hizo *check-in* en el restaurante chino Palitos", "Sebastián hizo *check-in* en el Caballito Shopping Center", leemos en nuestras redes sociales). Si mañana Ana está caminando por el barrio de Belgrano buscando un restaurante para comer con una amiga, abrirá su servicio de mapas y Palitos será la primera opción. Si mañana Sebastián busca dónde comprar un par de zapatillas nuevas, su mail recibirá una oferta imperdible para adquirirlas con su tarjeta de crédito que "casualmente" tendrá un 20% de descuento en el shopping de Caballito.

Netflix es otro ejemplo de cómo los metadatos de internet se utilizan

para detectar nuestros gustos y, en este caso, transformarlos en nuevos productos, por ejemplo, series o películas. Cada vez que le decimos al servicio de video que nos gustó tal película, la compartimos con nuestros amigos en las redes sociales, la calificamos con una estrellita o cinco, o simplemente buscamos "Kevin Spacey" para ver films de nuestro actor preferido, el servicio toma nota. También se nutre de lo que rastreamos en servicios de descargas "ilegales", como los de *torrents*, o de *streaming online*. De esas búsquedas también se obtienen datos según las preferencias de la gente en determinado mes, año, lugar en el mundo, edad, sexo. *House of Cards*, la serie dirigida por David Fincher, creada y producida íntegramente por Netflix, se nutrió de ese estudio de los gustos de sus suscriptores. Mal no le fue: la compañía ya acapara el 30% del tráfico de internet de Estados Unidos y tiene 50 millones de suscriptores en el mundo[188], y la serie va por su tercera temporada y ganó los premios más importantes de la industria del entretenimiento, entre ellos varios Globos de Oro y Premios Emmy.

Internet funciona como un escáner de preferencias, a medida que le damos (voluntaria o involuntariamente) nuestros datos a algunas grandes corporaciones que se encargan de analizar cada huella que dejamos, cobrar por publicidad a las empresas que quieren vendernos algo y de predecir lo que vamos a desear mañana. Entre esas enormes compañías están los buscadores como Google, Yahoo o Bing! (pero especialmente Google), las redes sociales (sobre todo Facebook, por su cantidad de usuarios), y toda una serie de de aplicaciones que utilizamos en nuestros móviles y van captando nuestra información.

Las bases de datos que se van conformando con las preferencias de los usuarios son el insumo más preciado de las empresas, tanto para ofrecernos hoy productos o servicios como para diseñar los que querremos comprar en el futuro. El análisis de esa gran cantidad de información, o *big data*[189], es un área a la que las empresas, a través de departamentos

[188] Según datos de julio de 2014.

[189] *Big data* es el área de la tecnología que procesa enormes cantidades de datos

de investigación y desarrollo, le dan cada vez más importancia. La célula básica de esa maquinaria somos nosotros, cómo nos movemos, nuestros gustos y preferencias. Y esos datos son valiosos. "En febrero de 2014 Facebook compró la empresa de mensajería WhatsApp por 19 mil millones de dólares. La cantidad de dinero mencionada puede cobrar cierto sentido si se la compara con los valores con que cotizan empresas como United Airlines (15 mil millones), Sony (17 mil millones) o Fiat Chrysler (12 mil millones). Estas tienen edificios, oficinas, fábricas, diseños, equipos de investigación y miles de trabajadores, pero valen menos que una aplicación, algunos servidores, una oficina y unos 50 empleados. ¿Qué estaba comprando Facebook realmente? La respuesta es: acceso a los cerca de 450 millones de usuarios de WhatsApp", explica el periodista Esteban Magnani[190].

El mercado de los datos es inmenso. En 2002, por primera vez en la historia, los humanos tuvieron más información almacenada de manera digital que en soportes analógicos. Cinco años más tarde ya casi el 95% de toda la información mundial era codificada digitalmente. Es decir, vivimos rodeados de datos, que nosotros mismos producimos cada vez que mandamos un mail, posteamos en una red social, buscamos en internet.

Google genera alrededor de 25 petabytes nuevos de información por

---

que van dejando ("voluntariamente", cuando aceptan los términos y condiciones) los usuarios a través de sus "huellas digitales *online*", con el diario uso de dispositivos, herramientas y plataformas digitales. Su utilización más extendida se aplica al marketing digital, para predecir deseos y gustos de los consumidores y ofrecerles productos y servicios orientados a su "*target*" o perfil de consumidor. En Europa, el 57% de los comercios ya utiliza algún sistema para procesar los datos que generan los 369 millones de internautas del continente. La contracara y frontera legal está en el consentimiento del consumidor (que haya aceptado brindar esa información) y en establecer tendencias o patrones —y no identificaciones personales— de un individuo en particular.

[190] Magnani, Esteban, Tensión en la red, 2014, disponible en http://www.estebanmagnani.com.ar/.

día (exactamente la misma cantidad de datos útiles generados por el LHC o Gran Colisionador de Hadrones en un año). En YouTube se sube una hora de videos nuevos por segundo. Hoy, en 2015, somos 6.500 millones de habitantes, conectados a 6.500 millones de equipos electrónicos. En 2020, seremos 8.000 millones de personas con 150 mil millones de objetos conectados, y habrá 57 bytes de información (o 57 caracteres —letras, números, emoticones—) por cada grano de arena en el mundo. Todos esos objetos conectados realizan acciones.Y esas acciones generan datos que no sólo circulan por la Red: esa información recorre cables con dueños y queda almacenada en servidores de empresas. Esa enorme masa de datos aumenta su valor a medida que crece en volumen. En 2012, era de 6 mil millones de dólares. En 2018, será de 48 mil millones.

El valor de la información varía según quién la utilice. Por un lado, existe un mercado negro de datos personales. Según un informe de la empresa de seguridad informática Symantec de principios de 2015, los precios rondaban, por ejemplo, entre los 2 y 12 dólares por cada mil seguidores de redes sociales, o los 70 y 150 dólares por un millón de direcciones de correo electrónico verificadas. Pero luego hay un gran mercado "legal" de datos donde las empresas invierten en acaparar y analizar información para, fundamentalmente, realizar ventas y ofrecer servicios. Cuando Facebook compró WhatsApp estaba adquiriendo, fundamentalmente, una base de datos de 450 millones de usuarios. En Estados Unidos, las grandes tiendas usan la información de sus clientes para vender productos cada vez mejor direccionados, también de acuerdo con los comportamientos de los usuarios en los sitios de comercio electrónico. En la Argentina, el 50% de las empresas afirma realizar algún tipo de monitoreo sobre los datos de los consumidores *online*, y ese porcentaje crece a medida que procesar los datos es cada vez menos costoso y las tecnologías para realizarlo más accesibles a una mayor cantidad de empresas.

Cuando Edward Snowden reveló que la Agencia Nacional de Seguridad espiaba masivamente a los ciudadanos de Estados Unidos y el mundo, no sólo descubrió públicamente lo que hacía esa agencia estatal. También mostró que otras empresas privadas cooperaban para inter-

ceptar las comunicaciones o accedían a algunos pedidos de vigilancia. Sin embargo, pocos pusieron el foco en las firmas privadas. La razón es sencilla: Google y otras empresas similares adquirieron un gran poder al resolvernos con sus servicios cosas importantes y útiles de nuestras vidas. También, invierten miles de millones en publicidad.

¿Somos todos tontos al dejar nuestros datos en manos de otros o de regalarlos a cambio de servicios gratuitos? No. Los beneficios existen. Pero cada uno de ellos también conlleva un peligro, una deuda: una cesión de datos.

A Instagram le damos nuestros datos a cambio de tomar fotografías, ponerles filtros y compartirlas. A Twitter le damos nuestra información de perfil, ubicación, gustos y amigos a cambio de conectarnos con otra gente, leer las noticias y opinar de cualquier cosa. A Foursquare le damos nuestra ubicación a cambio de compartir reseñas de lugares, restaurantes y decir que estuvimos allí. A Facebook le damos nuestros datos a cambio de demostrar lo geniales que somos, lo bien que la pasamos y ver lo que hacen los otros y lo geniales que son ellos también. A Amazon le damos los datos de lo que compramos y las opiniones sobre esos productos a cambio de encontrar el mayor supermercado del mundo y algunas buenas ofertas. A Medium o algunas plataformas de publicación de blogs les damos contenidos gratis a cambio de darnos exposición pública. A Google le damos nuestros datos para vendernos cosas y que otros nos vendan más cosas a cambio de tener mail, usar Google Docs, hacer búsquedas, usar su navegador Chrome, sus teléfonos Android, su plataforma Blogger, su sitio de videos YouTube, su calendario, sus mapas. Damos, damos, damos. Somos eternos donantes de datos.

Mientras aceptamos estos intercambios, estas empresas ganan dinero. Mucho. Facebook sin usuarios no sería Facebook, y Mark Zuckerberg, su dueño, no estaría en el puesto 16 de los hombres más ricos del mundo[191].

[191] Según datos de *Forbes*, de marzo de 2015, su riqueza supera los 33 mil millones de dólares.

Con más de 1.350 millones de usuarios activos (en octubre de 2014) la empresa tiene un valor de más de 100 mil millones de dólares. ¿Dónde reside este valor? En nosotros, los usuarios: cada vez que agregamos un amigo, posteamos un comentario, una nota, o una foto, generamos información, es decir, más valor. Lo mismo sucede con Google, la empresa de publicidad más grande del mundo, basada en que todos dejamos nuestras huellas de datos cuando usamos su buscador, el mail, los mapas o los documentos. En el mercado de los datos, como ocurre con otros mercados de la tecnología, esas ganancias también se la llevan unas pocas, grandes y súperricas empresas.

El tecnólogo y escritor Jaron Lanier llama a este esquema "el modelo de negocios del canto de sirenas"[192]. Según él, consiste en que estas pocas compañías "se quedan con toda la información posible y utilizan computadoras muy poderosas para obtener beneficios gigantes" en un formato que funciona haciendo que la gente les dé sus datos sin un beneficio monetario, sacándoselos subrepticiamente. Las empresas siempre ganan, nunca corren riesgos. Manejando esos detalles, pueden predecir las tendencias que tomarán las personas. "Por ejemplo, una compañía de seguros puede utilizar una gran cantidad de datos para solamente asegurar a quienes no vayan a enfermarse. El problema es que pueden hacerlo si tienen grandes computadoras para procesarlos. El resto deberá pagar por el riesgo". Para Lanier, el modelo funciona de manera brillante a corto plazo, es decir, en nuestra era, donde las grandes compañías como Google o Facebook se enriquecen, mientras siguen sumando servicios y personas a sus negocios. El problema es que, a largo plazo, esto nos lleva a otro problema de concentración del mercado de la tecnología. Y como la tecnología es cada vez más ubicua, no podemos escapar de ella para ninguna acción de nuestras vidas y tampoco podremos escapar del poder de estas empresas. Aún más: las corporaciones como Google tienen planes para llegar a cada vez más actividades y negocios: desde fabricar autos y ser dueños de la flota de drones más grandes del mundo hasta

[192] Lanier, Jaron. *¿Quién controla el futuro?*, Buenos Aires, Debate, 2015.

predecir las enfermedades futuras a partir de las palabras que la gente tipea en su buscador[193].

Para Lanier, la última y también grave consecuencia de este modelo ya no es sólo tecnológica. Es política y social. Porque estamos dando a estas pocas compañías el control de nuestro futuro. Pero también una serie infinita de negocios que hasta ahora están repartidos en otras empresas: las automotrices fabrican autos en el mundo; las farmacéuticas, remedios; las editoriales, libros. Ninguna de ellas es pobre ni hace beneficencia. ¿Pero qué ocurrirá si Google, por ejemplo, se hace fuerte en otra serie de industrias? ¿Qué pasará si, con internet.org[194], Facebook se convierte, además de dueño de la red social más poblada del planeta, en el principal proveedor de conectividad del mundo? Algunos dirán: es la competencia, es el libre mercado, es el darwinismo aplicado a los negocios, que siempre existió e hizo crecer al capitalismo. Otros sostendrán: todo cambio de época temió que una nueva casta de privilegiados se hiciera de todos los beneficios del nuevo modelo. Es cierto. Pero también somos nosotros quienes, en este caso, estamos ayudando masivamente, aceptando la tecnología sin crítica, a que el problema sea más que una decisión individual y se convierta en una cuestión colectiva.

¿Cómo contribuimos a incrementar este problema? Hay tres intercambios que, usados como ejemplos[195], pueden ofrecernos una nueva conciencia sobre el poder que dejamos en manos de otros.

[193] Días antes del pico de la gripe aviar en México en 2009, Google ya había registrado el incremento de las búsquedas y podía prever la llegada de la epidemia a ese país.

[194] Internet.org es una asociación entre Facebook y seis gigantes de la telefonía móvil. Lanzada en 2013, pretende llevar conectividad a los lugares del mundo todavía sin ella, pero a cambio de que todos los usuarios lo hagan "pasando" por su plataforma, y en cierto modo, por su negocio, con lo que generó grandes críticas desde su lanzamiento.

[195] Por supuesto, existen miles de otros en el mundo *online*, tanto o más peligrosos, pero nos centraremos en tres como ejemplos, dada la cantidad de usuarios que utilizan estos servicios en el mundo, y especialmente en Argentina.

El intercambio Google

Servicios útiles y "gratuitos" a cambio de publicidad

Google llegó a dominar internet como Julio César dominó Roma. Antes de él (de César y de Google) había un estado de caos. Roma tenía líderes débiles e ineficaces que no se ganaban el apoyo del pueblo ni lograban gobernar la ciudad. La Red, por su parte, era una colección de documentos asociados entre sí, pero desordenados, donde era imposible separar lo valioso de lo insignificante, lo cierto y lo falso. En medio de esa internet anárquica llegó Google. El 27 de septiembre de 1998, desde California, presentó un motor de búsqueda simple que clasificó el caos para los usuarios y dio el primer paso con el que sentó las bases de su actual imperio. El motor de búsqueda era limpio, puro y simple. No aceptaba dinero para situar una página adelante de otra en una búsqueda. El sitio más mencionado era el más relevante según los usuarios. Y lo mejor: funcionaba bien, cumplía su rol de editor en un mundo de anarquía. El secreto era que su técnica de búsqueda imitaba el modo en que el cerebro humano recuerda la información. Fue fácil adoptarlo porque entró en nuestra mente como una herramienta más, como una extensión de nuestros pensamientos. Desde allí, buscar es *googlear*, conocer es *googlear*, recordar es... *googlear*.

A partir de ese primer paso, Google construyó su imperio. Con esa metáfora histórica, Siva Vaidhyanathan, un analista de medios que escribe en las publicaciones más prestigiosas del mundo, sienta su tesis de *La googlización de todo*[196], un libro donde explica cómo llegamos a darle a la empresa de Sergei Brin y Larry Page[197] el control de nuestras vidas, casi sin percibirlo, pero con motivos que no se explican sólo por maldad o codicia capitalista. "Google domina la *Word Wide Web*. Pero jamás se llevó a cabo una votación para elegir quién la gobernaría. Ninguna entidad

[196] Vaidhyanathan, Siva. *La googlización de todo (y por qué deberíamos preocuparnos)*, Océano, México, 2010.

[197] En el puesto 19 y 20 de los más ricos del mundo, según *Forbes* (marzo de 2015).

nombró a Google su representante, procónsul o virrey. Esta compañía llenó sencillamente el vacío cuando no había ninguna otra autoridad", dice Vaidhyanathan, que no considera a la empresa ni buena ni mala, sino que busca desentrañar cuánto de sus reglas moldean hoy nuestras vidas, al menos para conocer esas implicancias. "Ahora permitimos a la compañía determinar qué es importante, relevante y cierto en la web y en el mundo. Confiamos en Google e, incluso, creemos que actúa en nuestro beneficio."

Google ocupó un lugar. Lo hizo bien. Se convirtió en la empresa más eficiente de la Red. Su enorme poder no es casual. Sin embargo, como todo dominio que crece en un terreno de necesidad y expande sus tentáculos planetariamente, sus riesgos también pueden ser importantes.

Según Vaidhyanathan, la *googlización* de nuestro mundo afecta tres grandes áreas de interés y de la conducta humana. El primero es el "nosotros": cómo Google influye en la información, los hábitos, las opiniones y los juicios personales. El segundo es el "mundo": la aceptación de un tipo de vigilancia parecida a un "imperialismo infraestructural", es decir, una empresa que sabe, mediante nuestro uso de la tecnología, prácticamente todo lo que sucede en el mundo, que tiene un mapa de información capaz de predecir enfermedades, guerras, gustos musicales, decisiones políticas.Y todo eso lo hace desde Mountain View, una ciudad del condado de Santa Clara, California, que es la sede mundial del poder: allí también tienen sus oficinas Adobe, AOL, Facebook, Linkedin, Microsoft, Nokia, Red Hat, Symantec, VeriSign, entre otras. En esos cuarteles generales, Google posee una red de información que haría las fantasías de cualquier jefe del ejército del planeta: fotos de cada rincón del mundo, los datos —demográficamente segmentados— de cada persona que utiliza sus servicios, la información —en tiempo real, también en un mapa preciso— de qué le importa a la gente en determinado momento a partir de las búsquedas. Su tercer dominio es "el conocimiento": Google tiene efectos poderosos sobre el uso del enorme conjunto de saberes acumulados en libros, bases de datos en línea y la Red.

¿Cómo llegamos a darle este dominio generalizado de nuestras vidas?

Cediendo partes crecientes de nuestro uso de internet a servicios como Gmail, YouTube, Google Maps, y las más de 150 empresas y aplicaciones que conforman su reino. La consecuencia es que en un tiempo (si ya no es así) la empresa estará a punto de volverse indistinguible de la internet misma. Pero como decía Spiderman (y antes había dicho Franklin Roosvelt): todo poder conlleva una gran responsabilidad. Y la eficiencia no nos permite ver que Google no es sólo virtudes. Lo dice Vaidhyanathan: "Resulta obvio que Google mejora nuestra vida, facilita nuestros proyectos y reduce nuestro mundo que no tomamos en cuenta los costos, riesgos, opciones y consecuencias duraderas de la optimista aceptación que le otorgamos". Por eso, dice el autor: "Cuestionar el papel de Google en nuestra vida y la fe que le tenemos no es fácil. Google hace mucho bien y poco daño a la mayoría de la gente".

Junto con el bien, la compañía de Mountain View se transformó en el principal filtro del universo. El problema es que no es un cristal transparente, sino más bien un anteojo con graduaciones que altera lo que creemos cierto o importante. Es un espejo que nos devuelve respuestas a nuestras preguntas, pero antes las clasifica, desde una visión del mundo: aquélla que construyeron un grupo de hombres y mujeres desde un lugar de California.

Pero la respuesta no es sólo técnica. Es —otra vez, como en las guerras de internet— económica.

Google es una compañía de publicidad. La más grande del mundo. Su modelo de negocios reside en tener la información más actualizada de sus usuarios —es decir, de nosotros—, que somos a su vez consumidores en miles de otros sitios. Le interesa saber no sólo qué hacemos, qué nos gusta y qué compramos hoy, sino qué vamos a querer hacer, qué nos va a gustar y por qué vamos a estar dispuestos a pagar mañana. Nos parece que la televisión, obligándonos a ver una publicidad en el corte, es una forma antigua de vendernos cosas y por eso apelamos al *zapping*. Pero Google lo hace todo el tiempo, ofreciéndonos y vendiéndonos lo que necesitamos (y lo que no) sin que seamos tan conscientes de ello.

El modelo de negocios de internet se basa en la publicidad: en miles

de millones de dólares[198] que se invierten para vincular a usuarios con perfiles determinados con las marcas o los productos con los que podrían estar interesados. Para eso, las empresas que venden esos anuncios, principalmente Google que controla un tercio de toda la publicidad digital del mundo y más de la mitad de móviles[199], tienen que conocernos. Cuantos más detalles sepan de nosotros más eficiente será su negocio y más dinero podrán ganar. Los ingresos de Google, de hecho, están compuestos en un 91% por ganancias de publicidad.

En internet todo puede medirse: si hicimos clic en un anuncio, si después de hacer clic comparamos entre dos productos y si finalmente compramos alguno. Cada paso está monitoreado. Tanto, que si ayer no nos decidimos entre un hotel u otro, mañana, sin recordar que ayer pensamos en el alojamiento de nuestras vacaciones, esa oferta de hoteles (o de otros) volverá. Google le cobra a las empresas por saber qué estamos buscando hoy, pero también porque tiene la información de lo que buscamos ayer y los sitios que visitamos, que probablemente le dará las claves de lo que buscaremos mañana. Para hacerlo, estas compañías (Google, Yahoo, Facebook) tienen que invadir nuestra privacidad. No existe otra forma de hacerlo. Pedirles que no lo hagan sería reclamarles algo imposible: que cambien el modelo de negocios que les hizo ganar
60 mil millones de dólares en 2013 (siete millones de dólares por hora, 168 mil por segundo) y que sus dueños, Sergei Brin y Larry Page, abandonen la lista de hombres más ricos del mundo, con casi 30 mil millones de dólares en su cuenta bancaria, cada uno.

¿Qué sabe Google de nosotros? Lo que quiere saber: qué nos interesa, qué necesitamos y en qué creemos (política, religión, espiritualidad). Lo hace a través de algunos de sus servicios: las búsquedas de Google, el navegador Chrome, el servicio de correo electrónico Gmail, los avisos publicitarios (Google Ads). Google sabe lo que hacemos *online*: dónde

[198] 137 mil millones de dólares en 2014.

[199] "Google, mighty now, but not forever", *The New York Times*, 11 de febrero de 2015: http://nyti.ms/1FeQaPy.

usamos la computadora, qué escribimos y leemos, qué miramos. Para eso tiene, además de los servicios principales, otros como Google News (una sección de noticias curadas por sus editores), la no tan popular red social Google+, Book Search (para buscar libros), Double Click (una empresa de publicidad), Google Docs (un archivo y repositorio de todo tipo de documentos, que además se pueden editar y compartir en línea) y las plataformas Blogger (de blogs), YouTube (de videos) y Google TV (una plataforma de televisión inteligente).

Google puede localizarnos: sabe dónde estuvimos, dónde queremos ir, dónde trabajamos o nos encontramos a tomar un café, dónde vivimos y con quién nos comunicamos. A través de las búsquedas o usando su navegador, por nuestros mails, por los chats (Hangouts), por lo que compartimos en Google+, por su servicio Street View, por el Calendario donde marcamos las reuniones a las que iremos y con quién iremos, por sus Mapas, al usar las funciones de geolocalización de Android y a través de su aplicación Waze (de tráfico y navegación). También qué decimos, a quién le hablamos, cómo es nuestra voz, qué idioma hablamos, cuántos mails enviamos y con quién, a qué días y horas lo hacemos, y qué decimos en esos mails. Sabe, además, lo que compramos, cuánto gastamos y cuándo lo hacemos, a través de servicios como Google Checkout, Wallet y Shopping.

Si usamos un teléfono Android, también puede acceder a nuestra lista de llamadas, mensajes y búsquedas *online*. Además, guarda los datos de nuestra IP (el número que identifica el dispositivo que nos está conectando a internet) por 9 meses y las cookies[200] por un año y medio, lo que le permite un tiempo más que extenso para analizar los

[200] Una cookie es una pequeña porción de información que envía un sitio web y queda almacenada en el navegador del usuario para que ese sitio pueda consultar la actividad previa de esa persona-computadora-usuario. Se utiliza para no tener que introducir cada vez los datos de registro, pero al mismo tiempo para controlar a los usuarios, ya que guarda la información de los hábitos de navegación, las páginas visitadas, etc. Las cookies son una herramienta vital en el mercado de la publicidad *online*, para conseguir y monitorear los hábitos de los usuarios.

metadatos. Aunque intentemos evitar el monitoreo y tengamos configuradas algunas herramientas de privacidad Google sabe de nosotros. Un ejercicio sencillo para demostrarlo es tipear en su navegador "Google's ad preferences tool" e ingresar a nuestro perfil. Allí veremos quiénes somos para el gran mercado de la publicidad. En mi caso, Google sabe que soy mujer, que tengo entre 35 y 44 años, que vivo en Buenos Aires, hablo español, y me gustan o interesan cosas como: las artes escénicas (sí: voy mucho al teatro), la informática y la electrónica (sí: trabajo de esto, Google), la casa y el jardín (sí: suelo buscar recetas para curar a mis plantas de algunos males), las noticias del mundo (sí: también es mi trabajo), la música rock, urbana y hip-hop, la política, las series dramáticas (sí: si son series sobre política, mejor), la venta de entradas de eventos (sí: últimamente compré muchas entradas *online*), las universidades, los libros y la literatura (sí, Google, soy una intelectual), y los tratamientos capilares (no recuerdo por qué, pero si Google lo dice, debo haber buscado algo para mi pelo).

Google es una red de compañías entre que hay más de 150 empresas[201] que fue comprando en la última década y que, asociadas entre sí, consiguen que casi nada de lo que hacemos quede por fuera de su dominio porque cubren todos los aspectos conectados de la vida de cualquier persona del mundo. Expandirse a nuestros cuerpos y ofrecernos conexión permanente para que nunca dejemos de conectarnos a sus servicios son los próximos pasos de la gran compañía. Así lo demuestran el desarrollo de objetos como Google Glass (los anteojos inteligentes que buscan reemplazar a los *smartphones*), programas como Behavio, que permite a las computadoras entender y reaccionar a los comportamientos de los usuarios y una serie de instalaciones y máquinas para ofrecer internet —directamente, sin recurrir a otros proveedores—, como los desarrollos que lleva a cabo Google Fiber (fibra óptica de altísima velocidad, 100 veces más que el promedio del mercado, en grandes ciudades), los drones

[201] Android, Picasa, Panoramio, Stackdriver, Admob, Doubleclick, Nest, Songza, YouTube, entre otras.

de Titan Aerospace (para proveer internet en áreas de baja cobertura) o Loon (globos aerostáticos para dar conexión en áreas alejadas).

Con ellos, los servicios de Google estarán cada vez más interconectados con otros objetos para que la compañía se transforme en nuestra infraestructura digital, tan indistinguible como el aire que nos rodea. Ya hoy podemos verlo: estamos esperando el tren, chequeamos el horario en que pasa en nuestro teléfono o reloj inteligente, miramos el mail de nuestro jefe, aceptamos una invitación a una reunión, vemos la lista de cosas a comprar antes de llegar a casa y las noticias de la tarde para estar al corriente en la próxima cena con amigos. Google es nuestro reloj, nuestro editor de noticias, nuestra secretaria, nuestra mascota. Todo lo que necesitamos él lo sabe. Tal vez, incluso, lo que no teníamos ganas de conocer o de recordar.

La *googlización* del mundo tiene dos grandes consecuencias. La primera: convertirnos en productos, ignorando el verdadero alcance de lo que la compañía conoce sobre nosotros. La segunda —menos tangible pero igualmente vital para nuestro futuro— es que impone un mundo cuyas opciones se limitan y deciden desde las oficinas de la gran corporación. Ambos problemas responden a la misma causa, que está en el origen del negocio de Google: la recolección masiva de información y su administración.

La primera consecuencia está asociada con la cantidad de datos masivos que Google maneja de nosotros. Y a que en esa vastedad de detalles se juega una parte de nuestra privacidad. "En su núcleo, las compañías como Google están en el mismo negocio que la NSA. Recolectan una gran cantidad de información sobre la gente, la guardan, la integran y la usan para predecir comportamientos individuales y colectivos, que luego pueden vender a publicistas y otros", escribió Julian Assange[202] al impulsar, en 2014, su cruzada contra la corporación liderada por Eric Schmidt. Según el líder de WikiLeaks, esta similitud convirtió a Google

[202] "Who should own the internet?", *The New York Times*, 4 de diciembre de 2014: http://nyti.ms/1HTlBPa.

en el socio natural de la NSA e hizo que fuera colaboradora del mega-programa de espionaje Prism. "Google es más poderoso que la Iglesia", dijo Assange en su recorrido virtual por el mundo para presentar *Cuando Google encontró a WikiLeaks*[203], donde, además de demostrar que lo que parece gratis no lo es tanto, también en ese mecanismo hay prácticas que cuestionaríamos a los poderes del Estado pero muchas veces dejamos pasar cuando son obra de las compañías privadas.

Como afirma el tecnólogo Evgeny Morozov, el éxito de Google consiste en que su sistema es cada vez más ubicuo: llena cada espacio de nuestra vida cotidiana (nos manda una alerta para salir de casa media hora antes de la próxima reunión de trabajo, nos avisa que nuestro último turno con el médico fue hace un año, nos muestra el nuevo restaurante del barrio porque el último mes nuestro GPS nos llevó muchas veces a comer por allí). El problema, afirma Morozov, es que "somos demasiado mezquinos para no usar servicios gratuitos subsidiados por publicidad". El peligro es que con esto le damos, enceguecidos por sus soluciones mágicas, un inmenso reservorio de datos que lo alimenta para transformarlo en un animal cada vez más grande. Y allí reside su poder hipnótico para la economía y la política: en sus bases de datos se puede saber tanto de la gente (de nosotros) que la tentación de tener a la compañía como aliada es inmensa. Sin embargo, en el medio queda atrapada nuestra privacidad, o al menos nuestra opción de decidir quiénes tienen acceso a esa información.

Mientras tanto, para Eric Schmidt, el tema es sencillo: "Si tenés algo que no querés que otro sepa tal vez no deberías estar haciéndolo en primer lugar. Si realmente querés tener ese tipo de privacidad, la realidad es que los buscadores —incluido Google— retienen esa información por un tiempo". Su declaración recurre a una falacia repetida: "La gente inocente no tiene nada que esconder". Pero el problema no es si somos inocentes o culpables, sino algo previo: la privacidad importa por sí misma, porque es un derecho como usuarios y como ciudadanos. Es la base para

[203] Capital Intelectual, Buenos Aires, 2014.

la libertad, para expresarnos, para opinar. Si supiéramos que todo lo que hacemos va a ser visto por todos no actuaríamos de la misma forma.

La segunda consecuencia de la *googlización* está relacionada con el "orden del mundo" que nos ofrece la compañía y que hace que nuestro ecosistema se vea cada vez más limitado por las búsquedas, opciones y preferencias de lo que hicimos una hora, un día o un año antes en internet. Nuestros perfiles nos condenan. Somos lo que fuimos antes y, en el futuro, cuando queramos descubrir algo nuevo por fuera de lo que ya venimos eligiendo será gradualmente más difícil. Así lo advierte la periodista inglesa Aleks Krotoski cuando habla del fin de la serendipia, una palabra que significa la capacidad de descubrir algo accidentalmente, por casualidad, mientras estábamos buscando otra cosa. Gran parte del progreso humano, creativo, o de las ciencias, se produce por efecto de estos hallazgos inesperados. Pero, para que suceda, tenemos que tener la capacidad de olvidar, reinventar, salirnos de las fronteras previstas. "Eric Schmidt, CEO de Google, declaró que quería que su empresa fuera no sólo un motor de búsqueda sino un motor de serendipia, es decir, que pudiera predecir lo que la gente iba a preguntarse. ¡Y me pareció escalofriante! Porque no se puede predecir. Es un fenómeno individual, que se produce por accidente, y que termina teniendo valor. Por eso hay que reclamar la serendipia y cuidarla de que sea totalmente direccionada por la tecnología: porque es importante para el progreso de la sociedad", me dijo Krotoski en su paso por Buenos Aires[204].

Existen miles de ejemplos sobre cómo el mundo se achica si le damos todo el poder a las mismas manos. Uno es la construcción de los mapas de Google y cómo ella afectará el espacio público tal como lo conocíamos, en el futuro. Pero, más aún, sobre cómo esa lógica, al limitar nuestras opciones, nos convierte en personas más previsibles y al mundo en un lugar con menos capacidad de cambio (ni que hablar de grandes revoluciones). Según Morozov, la cartografía que nos propone la empresa

[204] "Los riesgos del tecnofundamentalismo", *Revista Ñ*, 25 de enero de 2013, http://clar.in/1COOT1I.

es profundamente conservadora: "Ya que la lógica publicitaria es su negocio principal, la compañía no está realmente interesada en introducir novedades radicales a nuestras vidas. Para tener éxito con los publicitarios necesita convencerlos de que las visiones de sus consumidores son exactas y pueden generar predicciones sobre adónde queremos ir (o, para ese objetivo, dónde queremos cliquear). La mejor forma de hacerlo es transformarnos en criaturas altamente previsibles, limitando de manera artificial nuestras elecciones"[205].

Otra forma de hacerlo, señala Morozov, es hacer que todos vayamos a los mismos lugares, recomendándonos lo que otros amigos visitaron en el mapa, informándonos las actividades de nuestros contactos de Google Plus, o sugiriéndonos esos restaurantes adonde otros fueron. Claro que los ofrecimientos no están construidos sólo por lo que nuestros amigos eligieron, sino por una mezcla de esas preferencias ordenada por la publicidad que otros dueños de restaurantes o sus agencias de publicidad le pagan a la gran corporación para ser exhibidas como las mejores opciones. "Google prefiere un mundo en donde siempre vayamos a los tres mismos restaurantes, antes que en uno donde nuestras consecuencias sean difíciles de prever."

Morozov rescata una frase de Daniel Graf, el director de Google Maps para móviles: "Si mirás un mapa: ¿debería ser siempre igual para vos y para mí? No estoy seguro. Porque yo voy a lugares distintos que vos". Sin embargo, advierte Morozov, aunque es cierto que todos vamos a sitios diversos, la "personalización" debería tratarse justamente de eso: de que nuestro instinto, gustos o preferencias determinen adónde queremos ir mañana y la capacidad de que eso sea diferente de ayer. O que, si elegimos otro lugar, seamos conscientes de que ese ordenamiento del mundo está construido por un algoritmo que guió esa preferencia por nosotros, pero además la filtró de acuerdo con criterios publicitarios, con los cuales, al mismo tiempo, una empresa está ganando dinero.

Además de lo comercial, Google está modificando la ciudad, nuestra

[205] "My map or yours", *Slate*, 28 de mayo de 2013: http://slate.me/1CgySCM.

concepción del paisaje urbano tal como lo conocemos:"En el mundo de Google, el espacio público es algo que se asienta entre nuestra casa y los restaurantes mejor posicionados por las críticas, y a los cuales morimos por ir". El problema, en el final de esa lógica, es que la visión del mundo limita el rol fundamental que tienen el desorden, el caos y la novedad en nuestra experiencia como habitantes de las ciudades.

Esa limitación de la novedad, de la sorpresa y de encontrar lo que no pensábamos también se ve limitada en el rol de la gran corporación como editora de las noticias, especialmente a través de su servicio Google News, que ordena, filtra y edita por nosotros las novedades del mundo. Esta guerra llegó incluso a los tribunales europeos, cuando diarios y revistas de ese continente pidieron que Google les pagara por enlazar sus contenidos, que aparecían en su herramienta noticiosa con un título de la nota y un breve párrafo de la misma. En respuesta, Google dijo que el objetivo de News era llevar tráfico hacia los medios de comunicación, y que esto los favorecía en términos de tráficos, ya que no tenía la intención de retener visitas y, al contrario, dirigir a los usuarios a las respectivas fuentes. Los diarios insistieron en que, aun así, Google debía pagarles, ya que ellos eran los que estaban produciendo en sus redacciones la información.

En junio de 2014, medios alemanes demandaron a Google, que estableció que sólo iba a exhibir el título del artículo con un link a éste, sin citar nada ni mostrar imágenes. Sin embargo, tres semanas más tarde, los diarios decidieron volver atrás, dando un permiso gratuito al buscador para que los citara otra vez. Según algunos estudios, el tráfico desde Google News había descendido un 80%. El ejemplo es otro más de un servicio que, con su ubicuidad, genera una situación de monopolio, en este caso informativo. Si no pasa por Google, no lo vemos. Si no lo vemos, no existe. Pero si existe, Google gana dinero. El círculo parece difícil de evitar y tiene a todas las industrias en la disyuntiva: ¿sumarse al gran poder o luchar, al margen de él?

Para los usuarios la perspectiva es similar. El dilema, para nosotros, es si la solución se trata de dejar de usar Chrome, Gmail, Android, Google

Maps o Google Drive cuando nos hacen, efectivamente, la vida más fácil. La respuesta es que no es necesario, pero sí lo es saber cuáles son las consecuencias que tienen estos intercambios diarios. En el caso de las redes sociales, se suma otra negociación que puede ser peligrosa. Y allí no es por la eficiencia, sino por aspectos emocionales: ver qué hacen los otros, mostrarnos, conocer personas, buscar amor, explotar el ego.

El intercambio Facebook

Mirar y ser mirados a cambio de saber qué nos gusta (y filtrar nuestro mundo)

El 1º de diciembre de 2014, los muros de Facebook se poblaron de un mensaje misterioso que sin embargo todos pensaron que sería bueno compartir. Con terminología legal, los cuatro párrafos de la proclama, reclamaban que lo que cada uno publicaba desde ese momento en la red social era propiedad personal y que la empresa no tenía derechos sobre esos datos, fotos o textos. El pedido se basaba en que la compañía había optado por "incluir el software que permitirá el uso de mi información personal" y que, recurriendo al "código de la propiedad intelectual" cualquier uso que se hiciera de la información debía tener un consentimiento por escrito de su responsable. Entonces hacía un llamado: "Los que leen este texto pueden copiarlo y pegarlo en su muro de Facebook. Esto les permitirá ponerse bajo la protección de los derechos de autor. Por esta versión, le digo a Facebook que está estrictamente prohibido divulgar, copiar, distribuir, difundir, o tomar cualquier otra acción en mi contra sobre la base de este perfil y/o su contenido". Y adelantaba una sanción: "La violación de mi privacidad es castigada por la ley (UCC 1-308 1- 308 1-103 y el Estatuto de Roma)". Se invitaba entonces a todos los usuarios a publicar el texto y al final se advertía: "Si usted no ha publicado esta declaración al menos una vez estará tácitamente permitiendo el uso de elementos como sus fotos, así como la información contenida en la actualización de su perfil".

Cada vez que alguien reproducía el texto en su perfil, yo pasaba del

asombro o la sonrisa a la certeza de que, si tantas personas estaban seguras de podían hacer ese reclamo a Facebook, era porque la mayoría de los usuarios no conocen las condiciones que aceptan para participar en las redes sociales. Nadie lee los términos y condiciones, pero además somos ingenuos en suponer que lo que dicen puede proteger algo de nuestra privacidad. Pero además, la multiplicación de esos cuatro párrafos dejaba en claro que las empresas que manejan las redes son muy exitosas en que creamos que, cuando participamos en ellas, todavía somos los dueños de nuestros datos. Que todos compartieran ese reclamo significaba que todavía no hay conciencia de que, al ser parte de Facebook, formamos parte de una máquina publicitaria donde nuestros datos construyen perfiles de consumidores para vendernos productos a través de la publicidad en su propia plataforma o en otras relacionadas. Pero, aún más: al estar en ellas integramos estudios sofisticados que se realizan con los datos que les ofrecemos a través de nuestro comportamiento *online*.

¿Qué sabe y puede hacer Facebook de nosotros cuando aceptamos sus términos y condiciones?[206] Sabe dónde estamos, a través de la ubicación de nuestro dispositivo móvil. Recolecta información que le damos a otras empresas del grupo Facebook como Instagram o WhatsApp. Comparte nuestros datos con servicios de publicidad, medición y análisis, aclarando que siempre es información "que no permitan la identificación personal". También, con proveedores de servicios, por ejemplo, los de infraestructura técnica (los servidores donde se guardan los datos), aunque aclara que "estos socios deben cumplir estrictas obligaciones de confidencialidad". La red social recopila datos de pago como el número de nuestra tarjeta de crédito, la fecha de vencimiento, el código de seguridad y la información de facturación de pagos o transacciones realizadas a través de la empresa.

Facebook aclara que puede compartir nuestra información personal

[206] Según la política de privacidad que rige desde el 1º de enero de 2015. La información puede verse procesada para facilitar su comprensión en la página de la Dirección Nacional de Protección de Datos Personales: www.jus.gob.ar/datospersonales.

en respuesta a un requerimiento legal, como una orden de registro, orden judicial o citación de organismos, dentro o fuera de Estados Unidos. También puede acceder, conservar y compartir información cuando crea de buena fe que es necesario para evitar el fraude y otras actividades ilegales, para protegerse a ellos mismos o como parte de investigaciones gubernamentales. La compañía conserva información sobre las cuentas que se desactivan por incumplimiento de los términos de uso durante un año, como mínimo, para "evitar que se repitan conductas abusivas o infracciones a las condiciones de uso". Para sus usuarios, de cualquier parte del mundo, que quieran reclamarle algún aspecto de su política de privacidad, el domicilio de la empresa está fijado en Irlanda, en el número 4 de Gran Canal Square, en Dublín.

Facebook es, después de Google, el segundo sitio más visitado del mundo. Creado en 2004, hoy cuenta con 1.350 millones de usuarios en el mundo, la misma cantidad de habitantes que el país más poblado: China. A ellos se le suman los 300 millones de usuarios de Instagram y los 600 millones de WhatsApp, dos empresas que adquirió en 2012 y 2014, respectivamente. El negocio de Facebook es acumular usuarios que utilicen activamente los servicios, lo cual le garantiza tener perfiles actualizados, saber de qué hablan, qué les gusta, con quién y sobre qué interactúan. Cuando Mark Zuckerberg creó la plataforma en su habitación de la Universidad de Harvard, sabía que una red donde los estudiantes pudieran coquetear y conocerse entre sí tenía que ser exitosa. Su invento superó ese objetivo y hoy también es una plataforma de expresión artística, política, un lugar de encuentro social, familiar y profesional. Pero su función primitiva sigue siendo la base de su éxito: Facebook se trata de que nos vean y ver a los otros.

En ese intercambio emocional Facebook tiene la razón de su éxito. Suponemos que nuestras acciones están siendo "vistas" por alguien más que nuestros contactos. Podemos intuir que al usar su servicio "gratuito" y hacer clic en sus publicidades la empresa está ganando dinero: 60 centavos de dólar (multiplicados por 1.300 millones de usuarios que permanecen un promedio de 40 minutos diarios en la red, la ganancia

es millonaria). Intuimos que nada de lo que allí sucede es del todo privado. Sin embargo, en la negociación, preferimos *aceptar* sus condiciones y olvidar —o ignorar— las consecuencias.

No es sencillo culpar a los usuarios de caer en este canto de sirenas. Los "términos y condiciones" de los sitios de internet, las constituciones que determinan los derechos y las obligaciones dentro de esos espacios virtuales, son algo relativamente nuevo (en 1998 sólo el 14% de las web contaban con políticas de información). Pero, además, están construidos para proteger a los sitios, plataformas o aplicaciones, más que a los usuarios. Un estudio realizado por el escritor Marcus Moretti y el especialista en derechos digitales Michael Naughton sobre los 50 sitios más importantes de Estados Unidos determinó que, sumados, sus términos y condiciones ocuparían 145.641 palabras. Es decir, unas 250 carillas de Word. Pero, aún si los leyéramos, lo que encontraríamos serían una serie de precauciones legales para proteger a las empresas de juicios y multas, escritas con un lenguaje vago, para reducir sus riesgos. En el medio de esas palabras las empresas han ido introduciendo mecanismos que contribuyen a recabar información para la industria de la *big data*: hábitos de consumo, afiliaciones políticas, orientación sexual, creencias religiosas, historias médicas.

Aceptar los términos y condiciones de un sitio o una red social es lo mismo que firmar un contrato. Pero como requiere un paso tan sencillo como hacer clic no le damos la importancia necesaria. "Si Apple pusiera el texto completo de *Mi Lucha* de Hitler en los Términos de Servicio de iTunes igual lo aceptaríamos", bromeó el conductor y periodista norteamericano John Oliver[207]. Sin embargo, al hacerlo, estamos dando consenso a una situación en la que nos convertimos en consumidores no sólo de ese sitio, sino de todo un sistema de publicidad y servicios relacionados. Ése es uno de los grandes riesgos: con sólo decirnos que "otros sitios" usarán la información pueden hacer que sean muchos más. Por ejemplo, al aceptar las condiciones del sitio de noticias de *The*

[207] "Last Week Tonight with John Oliver: Net Neutrality": http://bit.ly/1GaCjs8.

Huffington Post otras treinta y tres compañías tienen acceso a nuestros datos, según Disconect App[208], una aplicación que permite bloquear los servicios de recolección de información de terceros. De los 50 sitios investigados por Moretti y Naughton, 48 recolectan datos para otros. Sólo nueve de ellos informan para quiénes. El resto, lo oculta a cada uno de sus usuarios que hace clic en *aceptar*.

Si quisiéramos leer los términos y condiciones de los sitios que usamos en un año tendríamos que dedicar entre 181 y 304 horas[209]. Y repetir este procedimiento todos los años, ya que la mayoría de los sitios renuevan sus condiciones. Desde las compañías esto es pura estrategia: si los textos son largos y aburridos, entonces los consumidores no se van a molestar en leerlos o cuestionarlos. Lo cierto es que, en todo sitio que nos ofrezca un producto o contenido gratuito, nuestros datos serán utilizados, desde Facebook hasta sitios de pornografía con millones de usuarios diarios, como Xvideos o RedTube, cuyas políticas de privacidad, si las leyéramos, nos harían pensar dos veces en el placer inmediato que ofrecen sus servicios.

Pero además de escribir textos complejos para explicar algo muy simple ("usaremos tus datos para venderte cosas o para darles tus datos a otras empresas para que lo hagan") las compañías como Facebook también estudian, a través de equipos propios de *big data*, los comportamientos de sus usuarios. Del tamaño de un país tan grande como China, Facebook es el laboratorio humano del comportamiento humano más extenso y diverso con que los investigadores pueden soñar. Si además esas personas permiten a la empresa que las estudien, el siguiente paso no debería sorprendernos.

Durante una semana de enero de 2012, el equipo de Facebook Data Science y un grupo de investigadores y científicos de la Universidad de Cornell llevaron adelante un estudio que luego fue publicado en la

[208] https://disconnect.me/.

[209] Según el estudio "The Cost of Reading Privacy Policies", de Aleecia M. McDonald y Lorrie Faith Cranor, http://bit.ly/1Ei7bEL.

prestigiosa revista *Procedimientos de la Academia Nacional de Ciencias*. Tomaron a 700 mil usuarios y los dividieron en dos grupos. Al primero le alteraron el algoritmo para que recibiera actualizaciones positivas, basadas en un filtro de palabras relacionadas (feliz, alegría, bueno). Al segundo, para leer lo contrario: noticias negativas, imágenes de tragedias, frases con la palabra "no". Al terminar la semana tomaron nota de qué posteaban los usuarios de uno y otro grupo. El resultado fue obvio: quienes habían recibido estímulos positivos, publicaban cosas felices, y viceversa. El problema es que ninguna de las personas sometidas al estudio fue avisada —explícitamente— de que estaba siendo parte de él.

En junio de 2014, dos años después de la investigación, la experiencia se hizo pública. De inmediato, los medios, las redes sociales y otros científicos se lanzaron a criticarlo. Y Facebook tuvo que salir a dar explicaciones. "La investigación se realizó solamente durante una semana y ningún dato utilizado estaba ligado a una persona en particular", dijo Isabel Hernández, vocera de Facebook. La empresa también se defendió diciendo que sólo se afectó al 0,04% de los usuarios y que su intención era mejorar el servicio para mostrar contenido más relevante.

El problema es que Facebook podía hacer este estudio, ya que sus usuarios lo habían autorizado cuando daban *aceptar* a los 9 mil caracteres (3 carillas de Word) de sus términos y condiciones. En todo ese palabrerío, la empresa mencionaba dos veces la palabra "investigación", informándoles que podían ser parte de experimentos. Sin embargo, la revista *Forbes* reveló que la palabra "investigación" fue recién incluida en mayo de 2012, cinco meses después del estudio. Y la comunidad científica aclaró: existen reglas estrictas para que los participantes de un estudio brinden un consentimiento informado ante cada procedimiento. No existe algo así como un "consenso general".

Pero Facebook no sólo hizo esta investigación. Su equipo de Data Science, un grupo de sociólogos e informáticos que se dedican a transformar la *big data* de la red en resultados sobre los comportamientos y las expectativas de los usuarios, trabaja "a plena luz del día", da entrevistas y publica sus estudios en los medios. Esta vez, en lugar de estudiar si los

enamorados bajan su nivel de interacción cuando se ponen de novios (algo que también habían hecho), alteró emociones sin consentimiento previo, algo con hipotéticas consecuencias (la depresión incrementa el riesgo cardíaco un 5%, por ejemplo). Cuando se conoció el estudio, el filósofo de la tecnología Jaron Lanier escribió en *The New York Times*: "Sería inimaginable que una empresa farmacéutica pudiera experimentar, aleatoriamente, con una droga, en cientos de miles de personas. Imaginen al investigador diciendo: ´Yo no sabía si te iba a afectar y no te molesté para hacerlo´".

La red social fue tan lejos que el profesor de la Universidad de Cornell Jeff Hancock, coautor del estudio, admitió a la revista *The Atlantic*: "El algoritmo de Facebook es algo raro que la gente no entiende. No lo hemos discutido mucho como sociedad. Hay un tema de confianza alrededor de las tecnologías". El argumento de Hancock es que hasta sus propios alumnos no entienden cómo funciona ni siquiera el algoritmo de Google.

La falta de "objetividad" de Google, y también de Facebook, es un aspecto a veces olvidado, pero que también se relaciona con el manejo que las empresas realizan de nuestros datos. Un objetivo vital de ambas compañías es que permanezcamos la mayor cantidad de tiempo posible en sus ecosistemas. De esa forma, ellas se aseguran ganancias superiores. Pero, para lograrlo, necesitan alterar el mundo, es decir, mostrarnos lo que queremos ver (en términos de sus algoritmos, lo más "relevante") durante más tiempo, rodearnos de estímulos agradables o al menos no conflictivos.

Ese mecanismo detectó el escritor y activista Eli Parisier cuando un día, al ingresar a su muro de Facebook, comenzó a ver que los comentarios de sus contactos con ideología conservadora estaban desapareciendo durante el agitado debate por la nueva ley de salud que impulsaba el presidente Barack Obama esos días. Él, un declarado progresista político, podría haberse alegrado de no leer toda clase de opiniones contrarias a su ideología. Sin embargo, decidió investigar y descubrió que Facebook había estado analizando que él hacía más veces clic en los links de sus

amigos progresistas, y que por lo tanto éstos empezaban a aparecer más: si él tendía a actuar más ante ese estímulo, la red social quería que él viera más de ese contenido que del de los conservadores. El problema es que no le consultó si él estaba de acuerdo con esa edición "invisible" y algorítmica de su mundo. Pero Facebook lo había hecho, y puede hacerlo, a partir de nuestro consenso. Google también: prueben buscar una palabra y pídanle a uno o dos amigos que también la busquen y les manden una captura de pantalla de los resultados. Todos recibirán respuestas diferentes. La razón es que Google, Facebook y muchos otros sitios saben desde dónde buscamos, qué pensamos, qué nos gusta, qué edad, sexo, religión y orientación política tenemos. Si no, no sería posible que cada uno reciba un resultado distinto. "No hay más un Google estándar", dice Eli Parisier, que a partir de su descubrimiento escribió *The Filter Buble*[210], donde explica que este mecanismo no sólo puede aplicarse a Google o Facebook, sino que es también utilizado por buscadores como Yahoo News o sitios de información como The Huffington Post o *The New York Times*.

El planteo de Parisier vuelve al problema de un mundo donde, a partir de los datos masivos que tienen las grandes empresa de tecnología sobre nosotros, el universo de lo que vemos, accedemos, leemos o podemos descubrir se reduce cada día a una serie de opciones más personalizadas pero también más restringidas. "La Red, que iba a permitir un mayor debate, que iba a contribuir con la democracia, resultó convertirse en lo contrario", advierte el escritor.

El concepto de la burbuja de filtros que construimos cuando aceptamos el dominio de los algoritmos sobre nuestros datos no queda entonces sólo en una decisión individual. Es, también, un problema colectivo. Pero requiere de algo fundamental: nuestro consenso. Al igual que con una democracia, primero se necesita que elijamos vivir en ella y quienes nos representarán. Luego, que aceptemos y cumplamos las reglas que la delimitan. En las redes sociales acontece algo parecido: son un espacio

[210] http://www.thefilterbubble.com/.

público donde lo que decimos o mostramos no sólo puede verlo cualquiera, sino que además tiene relevancia para lo que nosotros mismos veremos en el futuro. La responsabilidad, en ese y otros ámbitos de la vida digital, es nuestra, como ciudadanos de las redes, un espacio más que habitamos.

Pero allí anida uno de los grandes conflictos: cómo aplicar la responsabilidad y el control cuando podemos tener en la mano un aparato que nos resuelva todo con un par de clics. Eso también sucede con los teléfonos móviles y sus aplicaciones, que bajamos y utilizamos sin preguntarnos demasiado a dónde van los datos que les damos a sus dueños.

El intercambio móvil

Llevar una computadora a todos lados a cambio de saber todo de nosotros

En 2025, además de los 4.700 millones de usuarios de internet, habrá 150 mil millones de objetos conectados a la Red[211]: computadoras, heladeras, televisores, autos, ropa, casas. De todos esos aparatos, los teléfonos celulares son los más universales. No sólo todos tenemos uno, sino que además lo llevamos como una parte de nuestro cuerpo.Y a diferencia de la computadora, cuya función está quedando en el ámbito laboral, por nuestros móviles fluyen nuestros datos más personales. Por ellos circula la información que indica dónde estamos, con quién hablamos, qué buscamos, qué leemos, las imágenes, la música y los videos más íntimos. Entrar en nuestro teléfono es ingresar a nuestra vida y a nuestra mente.

Los celulares son el dispositivo de control perfecto de nuestra era. Sin embargo, aunque allí está todo sobre nosotros, les damos poca importancia a los datos privados que acumulan. Aún más: entendemos poco de cómo funcionan sus programas y aplicaciones. Saben más sobre nosotros que nosotros mismos, pero dejamos que ellos o sus fabricantes hagan lo que quieren. Instalamos, damos *aceptar*, los llenamos de datos. Sólo si

[211] Según el estudio Cyberspace 2015 de Microsoft Research: http://bit.ly/1xtyWHR.

lo perdemos o nos lo roban nos volvemos, por un momento, conscientes de cuánto de nuestras vidas hay en ellos.

Iván Arce apoya una taza llena de café negro en una mesa larga de la sala de reuniones de la Fundación Manuel Sadosky. Allí dirige desde hace tres años el programa de Seguridad en las Tecnologías de Información y la Comunicación, que vincula empresas, universidades y el Estado para capacitar recursos humanos locales en seguridad informática. De remera grande y cómoda y pantalones pegados a sus piernas largas y flacas, Arce no da nada por cierto cuando habla: todo para él puede ser de otra manera; necesita cuestionar antes de responder. Sus veinte años de trabajo en seguridad informática —como cofundador y líder de tecnología de una de las empresas del rubro más importantes del mundo— contribuyen a esa forma de percibir el mundo, donde todo requiere una explicación y un testeo antes de convertirse en verdad.

Para Arce, que dedicó su vida a hackear sistemas para encontrar vulnerabilidades y arreglar fallas, la tecnología nunca es neutra: Además de cumplir su función puede servir para defender o atacar a quien la emplea. Él sabe cómo se hace una cosa y otra. Y nada de lo que hoy es una preocupación reciente para los usuarios comunes de la informática —la privacidad, el uso de los datos, la posibilidad de acceder a nuestra información— para él es nuevo.

Arce respira profundo entre las frases y habla como en una conferencia: con silencios, encadenando lógicamente sus pensamientos, con tiempo. Y va paso a paso, también, cuando le propongo desentrañar los mecanismos que hacen que los teléfonos celulares se conviertan en los aparatos que más pueden conocer nuestras vidas.

—Este celular con sistema operativo Android —el más común que tenemos hoy en Argentina— es como tener una computadora y un módem juntos. Adentro, tiene muchos microprocesadores, con distintos programas corriendo. Cada uno está hecho por un fabricante distinto: el del hardware, el que hace los microprocesadores, el que realiza los programas, el que los integra, el del sistema operativo y todos los que hacen las aplicaciones de tu celular.

—Es decir, que cuando te comprás un celular ya estás interactuando con mucha gente.

—Exacto. Una gran diversidad de gente que "metió mano" en diversos lugares. Todos los teléfonos integran distintos fabricantes y proveedores. Si yo soy un atacante malévolo que quiero poner algo para vigilar personas, puedo hacerlo trabajando en la empresa que hace los microprocesadores que se utilizan en los controladores de placa de red, por decirte algún componente. Pero, además, vos después te bajás cualquier aplicación que te gusta sin preguntar quién la hizo y encima le das *aceptar* a todos los términos y condiciones.

—Pero Samsung, Motorola o cualquier fabricante de móviles, ¿no saben eso, no realizan controles de seguridad para que no suceda?

—Pueden saberlo, pero es imposible controlar toda la cadena de proveedores. Son cientos. Y miles de versiones, modelos y variantes de aparatos y programas.

—¿Por qué un fabricante de celulares querría acceder a tu teléfono?

—Para leer todos los datos que tenés ahí y espiar toda tu información.

—¿No se supone que quiere que confíes en su aparato para algo tan importante como comunicarte?

—Puede tener un interés de negocios ilegítimos en hacerlo. Puede obtener un montón de información de los usuarios: qué hacen, cuáles son sus hábitos de uso y de consumo. Pero también puede tener un interés legítimo en rastrear tus hábitos de uso para mejorar el dispositivo: entonces necesita "ver" qué tipeás o cómo usás la pantalla. La línea que demarca lo que es legítimo de lo que es ilegítimo en términos de negocio es muy difusa. Pueden decir que están monitoreando usuarios para mejorar un software que usás. Pero también para armar perfiles para después venderles publicidad. O para darle esa información a algún gobierno que la pida. Cualquiera de las tres opciones es posible. ¿Qué hacés vos para verificar que nadie esté abusando de tu datos personales?

—En principio, no confiar.

—No confiar igual es dejarlo en manos de otros. Con la seguridad informática hay tres caminos: mitigar el riesgo, transferirlo o aceptarlo. Mitigar es tomar alguna acción concreta: por ejemplo, encriptar el teléfono, descargarte alguna aplicación para verificar si te están espiando, controlar qué hacen las aplicaciones que te bajaste, revisar qué permisos les diste. Transferir el riesgo al Estado o al fabricante es que, si te das cuenta que no están protegiendo tus datos, les avises o les pidas explicaciones de qué están haciendo con tu información. Eso también es ocuparse activamente del problema. Si no hacés ninguna de esas dos cosas, estás aceptando el riesgo. No hacer nada es aceptar.

—¿Y qué deberíamos hacer los usuarios de celulares?

—Las tres cosas. El problema es que demanda un esfuerzo importante. En un mundo ideal, todos los usuarios de teléfonos celulares deberían preocuparse por su privacidad, encriptar las comunicaciones, los contenidos de su teléfono, verificar que los fabricantes no hagan suciedades, no instalar aplicaciones inseguras, no hacer clic en mails que mandan personas desconocidas.

—Después de las revelaciones de Snowden se comenzó a hablar mucho más de criptografía, de encriptar las comunicaciones.

—Encriptar es una de las herramientas de la seguridad y la privacidad, sí. Hay herramientas como Silence Circle Text Secure, navegadores como Tor, una larga lista de herramientas. Pero no es lo único que hay que hacer. También tenés que asegurarte de que tu computadora y tu celular sean seguros y de tener la disciplina para hacer las cosas bien siempre.

—Y dedicarle mucho tiempo a hacer todo esto.

—Sí. Si tu vida está en peligro si te capturan las comunicaciones, deberías destinarle tiempo. Pero, si no, también. De otra manera, aceptás las cosas como vienen dadas.

dar aceptar: google, facebook y whatsapp

El mundo que describe Iván Arce podría ser uno en donde vivir con paranoia sería normal. Sin embargo, como sucede con cualquier peligro, el miedo no soluciona sus causas. Desde que Edward Snowden le mostró al mundo que los ciudadanos de su país y el planeta estaban siendo espiados sin control, la primera reacción fue el terror de saberse monitoreado. Luego sobrevino una etapa de debate y de difusión de herramientas que los ciudadanos podemos adoptar para proteger nuestras comunicaciones.

Una parte de esta ola también estuvo teñida de un "marketing de la privacidad", donde empresas lanzaron productos y servicios más seguros para plegarse a la preocupación por el cuidado de nuestros datos. Entre otros, figuran Blackphone, un teléfono móvil que protege los datos de sus clientes; Qlink.it, un servicio para encriptar mensajes; nuevas versiones del navegador Firefox con elementos para reducir el rastreo de información; o una nueva serie de descargas del ya mencionado Tor, que ofrece opciones para una navegación más segura. También se incrementaron las descargas de Telegram, el servicio de mensajería desarrollado en Rusia con mayores recursos de seguridad que WhatsApp. Este mensajero, algunos servicios de Google y Yahoo sumaron —después de las revelaciones de espionaje del programa Prism— herramientas de privacidad y seguridad. El mismo Snowden recomendó utilizar RedPhone y Signal, dos aplicaciones para cifrar las llamadas en Android e iOS (el sistema operativo de Apple), respectivamente. También, el uso de Text Secure, como alternativa a las aplicaciones de mensajería como WhatsApp y Telegram. Y preferir Spider Oak, un servicio de almacenamiento en línea para reemplazar a Dropbox, que había sido indicada como unas de las empresas en colaborar con la NSA. La lista de opciones, la mayoría de ellas basadas en software libre y desarrollos en los márgenes de las corporaciones, se multiplicó.

Organizaciones de derechos fundamentales en internet como Access Now y la Electronic Frontier Foundation (EFF), entre otras, publican y actualizan herramientas y aplicaciones que permiten una protección de la privacidad. La EFF tiene un Kit de Autodefensa contra el Monitoreo, en español, en ssd.eff.org/es, con tutoriales y materiales traducidos.

Digital Defenders cuenta también con uno con distintos recursos para protegerse en digitaldefenders.org/digitalfirstaid/. Y el colectivo Tactical Technology también tiene su botiquín de primeros auxilios para proteger la privacidad en info.securityinabox.org/es. Cualquiera de estas herramientas, actualizadas con frecuencia y usadas en conjunto (en la computadora, el teléfono, las comunicaciones, las aplicaciones), son útiles. Pierden su efecto si protegemos un dispositivo como el celular, pero luego, por ejemplo, sincronizamos el mail con una tableta y allí no protegemos las comunicaciones o usamos otro navegador.

Para Arce, no hay un sistema de seguridad perfecto, sino que existen usuarios con distintas necesidades a proteger.

—Lo más importante no es qué herramienta uses, sino la conciencia y la disciplina. Es generar un entorno seguro para vos, pero saber que vos formás parte de redes, donde no sólo pueden espiarte a vos, sino a quienes tienen contacto con vos. Relajarte en tu seguridad puede tener consecuencias más o menos graves. Depende de qué sea relevante para vos y cuánto tiempo vas a dedicarle.

—Por ejemplo, en tu caso, ¿cuáles son tus necesidades y cómo las protegés?

—Yo no sincronizo mis cuentas, es decir, no conecto unas cuentas con otras. Sólo mando mensajes de SMS y los encripto con Text Secure. No uso mails en el teléfono; sólo lo hago en la computadora. No hago backups de contactos en la nube, y deshabilito backups automáticos. Si pierdo las cosas, es un riesgo, pero yo decido. Y hay cosas que estoy dispuesto a perder.

—¿Por ejemplo?

—No uso la mayoría de las redes sociales. Pero es lo que yo estoy dispuesto a hacer. Es como en la película *El Padrino*: a veces te querés salir de "un asunto" peligroso, pero después tenés que volver a entrar o alguien te hace volver a entrar y te lleva al peligro. Acá es lo mismo: es resistir esa ola que te lleva, saber que si no tenés esa disciplina vas a correr riesgos. Y bueno, tampoco estoy en el grupito de WhatsApp de

los padres del jardín de mi hija: me pierdo de enterarme de cosas allí, pero las pregunto en la puerta cuando la voy a buscar.

—*Bueno, no estar en el grupito de WhatsApp de padres del jardín tal vez es una ventaja...*

—Sí, quizá es una ventaja secundaria de proteger mi privacidad —se ríe el experto en seguridad informática, y por un momento deja su seriedad de especialista para convertirse en un padre moderno, pero no lo suficiente como para perder el control de su privacidad.

El manejo de la privacidad y de nuestros datos será una de las guerras de internet más importantes del futuro. Lo será para reclamar a empresas y gobiernos que no nos espíen o que, si lo hacen, nos dejen saberlo. Las batallas serán por nuestros derechos: para decidir con quién compartimos nuestros datos, quiénes los manejan y controlan o de quién queremos protegernos.

También somos nosotros los que corremos, cada día, la frontera de lo privado. Queremos, reclamamos y actuamos para ver más de los otros. En 2014, cuando WhatsApp incorporó un ícono de "doble visto" en forma de tildes azules, muchos usuarios lo festejaron: ahora iban a poder saber cuándo sus mensajes eran leídos. Podían reclamar ser vistos o ser ignorados. Cuando eso sucedió, yo desactivé esa opción para que nadie pudiera ver si yo leía o no un mensaje, pero eso también implicaba que yo tampoco viera si los otros leían mis comunicaciones. A los pocos minutos de cambiar la configuración por una más privada, recibí un comentario:

—¿Por qué desactivaste el visto? ¿No te interesa ver si leen tus mensajes? —me reclamó un contacto de mi lista, con sinceridad.

—No, no me interesa. Bueno, en realidad a veces sí me interesa o me da curiosidad. Pero si el precio de saber si me leen es dejar abierta mi propia privacidad, prefiero no hacerlo.

La privacidad no siempre existió tal como la conocemos hoy. Es una idea de la modernidad, que se asentó cuando, con la revolución industrial, las ciudades crecieron sobre las áreas rurales. Al estar unos más cerca de otros necesitamos marcar límites. Hoy la consideramos algo que siempre existió, pero es, en verdad, una idea reciente en la sociedad. Al mismo tiempo, cuando estábamos acostumbrándonos a ella, el concepto de lo privado cambió a partir de la convivencia de la tecnología en cada aspecto de la vida. Hasta hace algunos años, incluso, pensábamos que internet podía ser un ámbito distinto de la "vida real". Que lo *offline* y lo *online* eran posibles de separar. Hoy, esa idea también quedó vieja: sabemos que ni son diferenciables ni tampoco el espacio de la Red es privado.

Sin embargo, todavía le reclamamos a lo *online* cierta privacidad. No reconocemos, tampoco, que en ese territorio existen dueños. Que quienes interactuamos allí lo hacemos bajo las reglas de otros: las empresas que controlan esos espacios.

El filósofo Darío Sztajnszrajber ocupa una mesa doble en la confitería Las Violetas, muy concurrida durante una mañana de marzo en que Buenos Aires recobra el ritmo del comienzo de clases. En nuestro rectángulo, rodeados de otros comensales que desayunan, leen el diario o trabajan, la conversación con el filósofo es privada. Pero ya nada garantiza que alguno de nosotros termine la charla y tuitee una frase que dijimos, alguien nos saque una foto y la suba a una red social o que nuestros teléfonos estén registrando todo al tiempo qué hablamos, sin darnos cuenta.

—¿La tecnología siempre implica control? ¿Siempre quien tiene mis datos tiene un poder sobre mí?

—Siempre hubo formas de control y de recabar la información casi total de las personas. Sucedió en diferentes momentos, con tecnologías distintas. No es la primera vez que la tecnología genera control. Hoy, también, hay una relación simbiótica: hay más datos porque hay más tecnología y hay más tecnología porque hay más datos.

—¿Por qué le reclamamos al Estado que no nos espíe, pero no parece molestarnos que lo hagan las empresas?

—Hay parte de la sociedad que sigue creyendo en la transparencia del capitalismo y del liberalismo. Cuando no cuestionamos a Google, en realidad no cuestionamos al mercado. Pero sí cuestionamos al Estado porque, según la idea liberal, el Estado manipula la libertad individual.

—Pero está la idea de que "tenemos menos privacidad", podemos ir por la calle y ser filmados por una cámara o que alguien nos saque una foto y la suba a una red social.

—Es que todo está relacionado con el contexto en que se da. Esa idea, hace cincuenta años, no hubiera tenido sentido, porque no estaban dadas las condiciones materiales, tecnológicas, para que sucediera. Si lo analizamos sin ese contexto, siempre lo vamos a ver como una pérdida o una degradación. Yo me peleo con esas posturas que ven que el mundo actual es un mundo que está perdiendo ciertos valores. Porque los valores no existen; son una construcción de la época. Hoy las formas de privacidad se "transformaron", no diría que se "perdieron". Se transformaron, porque hay otras también.

—Las categorías llegan después de los cambios.

—Exacto. Las instituciones siempre llegan tarde y las categorías explicativas, peor. Nos cuesta entender cómo la revolución tecnológica va minando de raíz las categorías con las que venimos pensando una realidad material diferente. ¿Sirve seguir hablando de identidad o de privacidad, en el mundo de las redes? Yo digo que no. No en la forma en que definimos lo privado y lo público o definimos identidad, por los menos en el siglo XX. ¿Qué sería lo privado y lo público en una red? Volver a pensar categorías es lo que más nos cuesta. Me parece que el gran drama con las transformaciones tecnológicas es ése. Es algo que pasó siempre, pero ahora el cambio va mucho más rápido. Obvio que hay gente que necesita seguir pensando la realidad con algunas categorías de verdad. Pero también hay mucha gente que necesita seguir creyendo en Dios.

Las guerras de internet también se tratan de eso: de qué intercambios hacemos para convivir con unas tecnologías que alteran nuestros hábitos, nuestras relaciones con los demás y el control de nuestros derechos. Pero mientras negociamos esos límites en forma privada, también formamos parte una sociedad que va cambiando sus formas. Y somos ciudadanos que construimos, con nuestras acciones, los derechos colectivos.

Las revelaciones sobre espionaje masivo que dio a conocer Edward Snowden en 2013 hicieron más visible un tema que ya preocupaba a especialistas en derechos de internet, académicos, gobiernos y activistas: quién controla nuestros datos y hasta donde la privacidad puede existir en la era digital.

En respuesta al problema, un grupo extremo propone dejar de usar internet porque estar en ella nunca es privado. En el otro extremo, están quienes la usan sin ningún cuidado: son aquellos que sostienen el argumento de que no tienen nada que esconder y, por lo tanto, nadie va a espiarlos. La tercera opción, que es la intermedia y más compleja de concretar, requiere compromiso y trabajo de nuestra parte: partir de la base de que nuestros datos ya no son privados y tomar algunas medidas al respecto, no solo como individuos aislados sino como parte de una sociedad.

En lo personal, el cuidado de nuestra privacidad con herramientas de encriptación, navegación anónima, el uso de sistemas operativos abiertos o productos que nos brinden información respecto de cómo están construidos o cómo manejan nuestros datos, son todas formas de ocuparnos del tema. Todas requieren tiempo, disciplina y compromiso. También que compartamos los conocimientos con otros, para generar el cambio y la adopción de esas herramientas por parte de quienes todavía no las utilizan. Sentarse un momento, una hora o incluso dos, con un amigo, un familiar o un colega, a explicarle cómo funcionan "las cosas" (en este caso, la tecnología) es un acto político, de expansión de derechos, porque permite ser más conscientes de lo que usamos y no adoptar

soluciones empaquetadas por otros. Si cuando vamos al supermercado no compramos productos muy caros en señal de protesta, si reclamamos a nuestra comuna que reparen una vereda o salimos a pedir a una manifestación un cambio político, deberíamos también generar acciones concretas respecto de nuestro uso de la tecnología. Si no lo hacemos, estaremos dejando que las cosas sigan como están.

Mientras tanto, en el mundo, se proponen soluciones para enfrentar o lidiar con los temas de privacidad.

La primera es una respuesta económica y propone que, ya que de todas formas nuestros datos serán usados por las empresas, que ellas nos paguen por hacerlo. La empresa Datacoup[212], por ejemplo, se presenta como una plataforma donde podemos ofrecer todos los accesos a nuestras cuentas, redes sociales y aplicaciones, y ganar dinero para que se utilice la información que hoy en día esas compañías utilizan sin compensarnos por ello. Existe un movimiento a favor de esta opción que está creciendo en el mundo, sobre la base de "si me van a espiar, por lo menos páguenme". Sin embargo, es una decisión peligrosa, porque su cimiento es aceptar la recopilación masiva de información y legitimarla. Es como la prostitución legal: que sea en Ámsterdan, con profesionales del sexo y en lugares limpios, no hace que no sea una explotación del cuerpo de otro. Además, la solución incrementa la desigualdad, porque no hace más que darle de comer al monstruo que se alimenta de los datos. Entonces, quienes más cuentas o datos tengan, ganarán más dinero, mientras que los que ya tienen menos, quedarán más al margen. Finalmente, tampoco resuelve qué pasaría con quienes no quieran vender sus datos a cambio del beneficio económico: ¿serán marginados de internet?

La segunda es la solución política, y es la que preferimos. Se trata de tomar a la privacidad no como un fin en sí mismo ("la privacidad está bien porque sí"), sino como un medio para otro fin más importante: vivir en un sistema democrático, donde podamos optar. Sin espacios privados, donde un algoritmo no decida por nosotros si quiere monitorearnos,

[212] http://datacoup.com/.

o donde estemos obligados a vender nuestros datos como mal menor a que igual los recolecten, no seremos ciudadanos completos. Para que las democracias sean realmente efectivas, necesitan que podamos negarnos a ciertas decisiones, que tengamos la capacidad de sabotear el sistema, de no aceptar las cosas tal como son dadas, sino cuestionarlas en caso de que estemos en desacuerdo con ellas. Si los aparatos y las aplicaciones nos proponen acompañarnos a todos lados, registrar nuestras pulsaciones, calorías, los lugares que visitamos y con quiénes conversamos, deberíamos también poder elegir entre otros que no lo hagan o prescindir de aquellos que lo hacen.

Esta opción no es fácil. Implica entender internet —y a la tecnología— sin ingenuidad. Significa no pedirle que resuelva todos los problemas por nosotros. Si dejamos que Google, nuestro proveedor de internet, los dueños de las redes sociales, las "nubes" donde guardamos los datos y los servicios de mensajería se encarguen de nuestras vidas porque es más fácil y nos ahorra tiempo, estamos cediendo un gran poder en sus manos. Es como elegir un presidente, un gobernador o un diputado y permitir que actúe sin control durante los cuatro años que dura su mandato. Es delegar todo en manos de otros para no ocuparnos nosotros. Ahora, si algo sale mal, ¿cómo reclamar después si no nos importó en su momento? Con la tecnología sucede lo mismo que con la representación política: ella siempre va a avanzar si la dejamos. La única forma de que no lo haga siempre para el mismo lugar (como otra forma de capitalismo concentrado) es entenderla, para ponerle límites, reclamarlos o construirlos colectivamente.

Desde este punto de vista político, la privacidad "en sí" no es el problema. Lo es, en cambio, el control de la privacidad. Quién monitorea mi información, cómo lo hace, con qué herramientas, informándome o no, son las preguntas que debemos hacernos. Porque allí —en reconocer a los poderes que controlan nuestros datos, cuánto ganan, para qué lo hacen— estaremos sabiendo más del mundo que nos rodea, en este caso en forma de tecnologías que deciden sobre nuestra vida.

Nuestros datos son más que unos y ceros. Son nuestras vidas, historias

personales, lo que queremos, lo que soñamos. La privacidad depende de cada uno. Es una lucha política que requiere involucrarse. La otra opción es elegir por la eficiencia, los intercambios para hacer las cosas más fáciles o más rápidas, y olvidarnos de las consecuencias. Si ésa es la decisión, entonces será lógico entregar nuestros datos a las empresas que nos prometan que en sus manos obtendremos beneficios. Si lo hacemos, debemos saber que les estamos dejando ese lugar a ellos porque nos resulta costoso ocuparlo: porque no tenemos tiempo, porque no nos dan ganas, porque preferimos ocuparnos de otras cosas.

Esa opción, la de no ocuparnos, también es una elección política. No controlar nuestra privacidad y nuestros datos nosotros mismos implica cedernos a otros. En esa antipolítica, habrá otros que harán política o negocios con nuestra información. Sin embargo, existe otra alternativa, la misma que nos hace salir a la calle a reclamar por algo que nos preocupa o a defender algo que queremos. La misma que nos hace participar en nuestro consorcio, organización social o comunidad. En la tecnología y en las guerras de internet también hay —y habrá— batallas por pelear, territorios en disputa por defender. Depende de nosotros tomar las armas y salir a ocupar esos espacios.