3
Vigilancia

> El utópico, inmanente y constantemente frustrado objeto del estado moderno es reducir la caótica, desordenada y eternamente cambiante realidad social subyacente en algo que se parezca a la plantilla administrativa de sus observaciones.
>
> JAMES C. SCOTT, *Seing Like a State*

Como cualquier narrativa distópica, todo empieza con un buen propósito. Dos amigos y estudiantes de doctorado llamados Lawrence Page y Serguéi Brin tratan de mejorar el buscador de la Biblioteca Digital del Departamento de Informática de la Universidad de Standford. Quieren implementar un sistema que «entienda exactamente lo que preguntas y te conteste exactamente lo que tú quieres», estableciendo una jerarquía en los resultados de cada búsqueda, priorizando los textos más citados y los autores más reputados. No hay héroe sin obstáculo. La capacidad máxima de los discos duros en 1996 era de cuatro gigabytes, muy poca capacidad para poder testar su algoritmo. Cuenta la leyenda que construyeron un servidor con bloques de Lego y encajaron allí diez discos de cuatro gigabytes en batería, con sus respectivos ventiladores. Aquel primer servidor de colorines, el origen del universo Alphabet INC., es hoy parte de la exposición permanente del Centro de Ingeniería Jen-Hsun Huang de Standford, frente a la reconstrucción del garaje donde William Hewlett y David Packard fundaron su compañía en 1939. «No tenían mucho —dice la nota de Hewlett-Packard—, poco más de quinientos dólares y un taladro de segunda mano». Larry y Serguéi tuvieron más ayuda. Concretamente una beca de la NSF/DARPA, cuyo origen es un programa del Departamento de Inteligencia estadounidense llamado Massive Digital Data Systems Project (MDDS).

El MDDS estaba capitaneado por la CIA y la NSA, pero gestionado por la National Science Foundation. A través de la NSF, habían repartido millones

de dólares en una docena de universidades de élite, entre ellas Stanford, CalTech, MIT, Carnegie Mellon y Harvard. «No solo las actividades [de la agencia] se han vuelto más complejas —dice el documento original del programa MDDS—, pero las necesidades cambiantes requieren que la IC [comunidad de inteligencia] procese distintas clases y grandes volúmenes de datos. En consecuencia, la IC ha decidido asumir un papel proactivo estimulando la investigación en la gestión de bases de datos masivas y asegurándose de que las necesidades de la IC pueden ser incorporadas o adaptadas a los productos comerciales». Las agencias buscaban un sistema de reconocimiento de patrones que les permitiera identificar personas «de interés» en la World Wide Web. Querían rastrear las comunicaciones y movimientos de todos los usuarios y registrar su «huella digital» para poder encontrar «pájaros de la misma pluma». Según el proverbio, las aves de la misma especie vuelan de la misma forma.[1] Si, pongamos por caso, un terrorista o disidente muestra determinados patrones, todas las personas con patrones similares debían ser identificadas cuanto antes, y vigiladas como posibles terroristas. Financiando su desarrollo, no solo se aseguran de que exista esta tecnología, sino también de que integre todas sus necesidades. Hoy, la NSF financia el 90 por ciento de la investigación universitaria de ciencias computacionales.

La Segunda Guerra Mundial fue el principio de un fructífero matrimonio entre la comunidad científica y la militar en Estados Unidos. Primero, fue la carrera por descifrar las comunicaciones de los alemanes y japoneses; después, por desarrollar la primera bomba atómica. El esfuerzo bélico produjo fuertes lazos económicos entre el Departamento de Defensa y los laboratorios universitarios, por no mencionar la cantidad de fichajes estelares que les brindó la migración masiva de científicos desde Europa. El origen de ARPA, la Agencia de Proyectos de Investigación Avanzados que creó ARPANET, había sido un vanguardista sistema de estaciones de radar computarizado en tiempo real diseñado por el MIT para alertar de un posible ataque soviético desde la distancia. Se llamaba SAGE (Semi Automatic Ground Enviroment). Participaron cuatro empresas: IBM hizo los sistemas de computación, Burroughs las comunicaciones, Western Electric diseñó y construyó las veintitrés torres de control y el Laboratorio Lincoln hizo la integración del sistema.

El desarrollo de SAGE concluyó en 1963. Era un proyecto de integración de sistemas extremadamente ambicioso, costó más que el proyecto Manhattan e inspiró algunas de las películas más icónicas de la época, como *Dr.*

Strangelove. Tenía veinticuatro centros de mando y tres centros de combate distribuidos por Estados Unidos. Cada puesto estaba conectado por líneas telefónicas a un centenar de elementos de defensa aérea que interactuaban entre sí. Lamentablemente, cuando se terminó de construir ya estaba obsoleto. Su única habilidad era alertar de la presencia de bombarderos en el espacio aéreo. Cuando la Unión Soviética puso en órbita el Sputnik 1, Estados Unidos comprendió que su modelo de vigilancia por control remoto tenía que abarcar países enteros, grupos políticos, manifestaciones. «Insurgentes». El Pentágono quería tener ojos y oídos en todas partes. El mundo entero era una zona de conflicto a vigilar. La victoria de la Revolución cubana había contagiado al resto de los países latinoamericanos con el apoyo económico y político de la Unión Soviética. También estaba el proceso de independencia de las colonias del sudeste asiático y su lamentable papel en Vietnam. La nueva tecnología de vigilancia remota tenía que ser capaz de observar todos estos «problemas» como procesos mecánicos predecibles, susceptibles de ser identificados y corregidos a tiempo. «Parecía una idea progresista —explica Yasha Levine, autor de *Surveillance Valley. The Secret Military History of the Internet*—. Era mejor que bombardear a esa gente. Con una cantidad de datos suficiente, podías arreglar el mundo sin derramar sangre». Lo que no se dejara corregir podía ser destruido desde la distancia, de manera rápida, limpia y eficaz.

El cerebro de ARPA era un *think tank* de cuarenta y cinco genios procedentes de las mejores universidades del país que se reunían cada seis semanas en La Jolla, California. Los llamaban los Jasones (por Jasón y los Argonautas). Dicen que eran casi todos físicos, que muchos venían del proyecto Manhattan, y aunque formaran un grupo secreto, es casi seguro que eran todos hombres y blancos. Suya fue la idea de plantar una red distribuida de sensores inalámbricos en la selva de Vietnam para identificar las rutas de suministro del Viet Cong y bombardearlas antes de que pudieran cumplir su función. Lo llamaron la Barrera electrónica de la Línea McNamara. Las señales eran procesadas en la base aérea de Nakhon Pathom, en Tailandia, en un centro de control equipado con terminales IBM 360 que hacían los mapas para las tropas aéreas.[2] «Habíamos cableado la ruta de Ho Chi Minh Trail como su fuera una máquina de pinball —contaba más tarde uno de los pilotos en el *Armed Forces Journal*—. La enchufábamos cada noche». Aún no se habían inventado los videojuegos. La operación se llamó *Igloo White*.

El concepto era una guerra sin bajas, desde el puesto de control. «En la guerra del futuro —declaraba en su discurso William Westmoreland,

comandante en jefe de las operaciones militares en Vietnam—, las fuerzas enemigas serán localizadas, rastreadas y disparadas de manera casi instantánea a través de enlaces de datos, evaluación computarizada asistida y sistemas de disparo automático». La idea ya estaba bien clara, pero la tecnología no. Los sensores solo podían comunicarse con el centro de control a través de los bombarderos, que hacían al mismo tiempo de router de los datos y de ejecutor. El Viet Cong aprendió rápidamente a engañarlos con señales falsas, haciéndoles lanzar bombas en lugares donde no había nada. La batería era extremadamente limitada, aunque casi daba igual, porque la mayor parte de los sensores se rompían nada más chocar contra el suelo. Sin embargo, en el proceso el departamento apoyó económicamente a las universidades y a las grandes tecnológicas (Texas Instruments, Magnavox, General Electric, Western Electric) en el desarrollo y fabricación de todo tipo de sensores: acústicos, sísmicos, químicos y de radiofrecuencia. Cuando acabó la guerra, toda aquella tecnología fue reciclada como sistema de vigilancia de la frontera con México. Y también para controlar a sus propios insurgentes, los millones de estadounidenses que se manifestaban contra la guerra de Vietnam y a favor de los derechos humanos de los vietnamitas. O en el caso de los movimientos afroamericanos, de sus propios derechos civiles.

Hay ahí un patrón que se repetirá de manera regular y predecible: toda tecnología desarrollada para luchar contra el terrorismo y por la libertad en otros países acaba formando parte del aparato de vigilancia doméstico, con la misma rapidez con que las latas que Nicolás-François Appert diseñó para el ejército de Napoleón acabaron en el mercado de París, alimentando civiles. Todas las tecnologías de vigilancia implementadas bajo secreto de Inteligencia o con ayuda del Gobierno federal son parte del aparato de vigilancia del Estado, aunque no pertenezcan a la institución. Si alguien pensaba que la privatización de la red significaba la desmilitarización de sus infraestructuras, estaba muy equivocado. Como dice el periodista Mark Ames, «el Pentágono inventó internet para ser la máquina de vigilancia perfecta. La vigilancia está grabada a fuego en su ADN». El ataque a las Torres Gemelas del 11 de septiembre de 2001 justificó importantes cambios en la legislación que formalizaron su condición primigenia. Seis meses después del atentado, la Patriot Act puso todas las infraestructuras de comunicaciones estadounidenses en manos de las agencias de inteligencia, incluida la incipiente industria de servicios online y su enorme banco de datos. El Departamento de Defensa quería extender sus largos tentáculos

hasta el último rincón de la vida del último usuario activo de internet. No tuvieron que hacer mucho esfuerzo. Gracias a la red social, tenían todo el trabajo hecho.

El pecado original de internet

Larry Page y Serguéi Brin lanzaron su buscador en 1998, desde el garaje de Susan Wojcicki en Menlo Park.[3] A finales de año, ya habían indexado dos millones y medio de webs. La sencillez de su página y su habilidad para filtrar la pornografía y el spam de sus resultados acabó limpiamente con el resto de buscadores: AltaVista, Lycos, Ask Jeeves y MSN Search, de Microsoft. Cuando estalló la burbuja les iba tan bien que se mudaron al bloque de edificios de Mountain View donde aún permanecen, y que ahora tiene un nombre: Googleplex. Su objetivo oficial ha sido «organizar la información del mundo y hacerla universalmente accesible y útil». Su código deontológico: «Don't do Evil» («no hagas el mal»). Su método: ofrecer servicios gratis a cambio de datos que son utilizados para mejorar el servicio. Sabiendo quién es el usuario podemos ofrecerle mejores resultados. Y, naturalmente, mejor publicidad.

Su siguiente gran *éxito* después de las búsquedas fue Gmail. En los términos de uso, Google se reserva el derecho de escanear y almacenar el contenido de los correos, incluso después de que el usuario los haya eliminado de la bandeja. En el mundo de las plataformas digitales nada muere ni desaparece, todo es material. Cuando lanzaron sus primeras aplicaciones para la nube —Google Docs y Google Sheets— los términos de uso originales se adjudicaban el derecho eterno de explotación de todo el contenido aportado por los usuarios, incluso después de haber eliminado sus cuentas. En 2002 compraron Pyra Labs, la empresa responsable de Blogger, la plataforma que democratiza la blogosfera. En 2003, en pleno auge blogosférico, Google lanza Adsense, una plataforma de banners publicitarios para la web que se extiende por miles de millones de páginas, desde las grandes cabeceras de periódicos internacionales hasta los blogs de poesía de los adolescentes suecos. Los banners de Adsense son «gratis», no requieren agencias de marketing ni programadores. Basta con meter un trocito de HTML en el código de la página y empezar a cobrar. Además, son inteligentes, lo que entonces significaba que los anuncios cambiaban en función del contenido que tenían alrededor. El foro de coches anuncia cosas de coches; el blog de recetas, gadgets de cocina, etcétera. Para «analizar» el

contenido, los Términos de Usuario de Google obtenían permiso para extraer los datos de la página y de cada uno de sus visitantes, incluyendo su IP, navegador, equipo informático y sus estadísticas en la página. Por ejemplo, qué está leyendo o dónde pincha. La mayor parte de los visitantes tenían cookies de Google, un trocito de código que se «pega» al navegador cuando navegas y te identifica de manera única. Gracias a la combinación de cookies y Adsense, Google podía seguir a un usuario de página en página y recoger información bajo una identificación de usuario o User ID. Los anuncios inteligentes ya no solo cambiarían en función de la web sino de lo que sabía Google sobre el usuario. Lo mismo con los resultados de las búsquedas de Google. Este sencillo mecanismo es el origen del ecosistema que los académicos, tecnólogos y analistas empiezan a llamar «Economía de la vigilancia», «capitalismo de plataformas», y «Feudalismo Digital».

A Serguéi Brin le gusta decir que se ha hecho rico ayudando a millones de personas a hacer las cosas que quieren hacer. Esto es completamente cierto. Todos los servicios de la empresa son excepcionales. Son útiles, fáciles de usar y ofrecen una nueva relación con el mundo y el espacio. También es cierto que todos están diseñados para la extracción masiva de datos: todo lo que busca, escribe, envía, calcula, recibe, pincha, comparte, lee, borra o adjunta el usuario es digerido por los algoritmos de Google y almacenado en sus servidores para la explotación eterna. Al principio de todo existía el concepto de que esta información no podía estar vinculada al mundo real. El User ID pertenecía al «mundo digital» de la plataforma y no estaba vinculado a una persona real en el mapa. Después llegaron Google Maps y Google Earth, un modelo de la Tierra creado a partir de un collage de imágenes satelitales, fotografías aéreas y datos SIG, financiado por el programa In-Q-Tel de la CIA.[4] Y, como complemento, un modelo literal a escala del mundo real llamado Google Street View.

Entre 2008 y 2010, los coches de Google salieron a fotografiar las calles de más de treinta países, incluyendo las fachadas de las casas adyacentes. Algunos vecinos se quejaron de que las cámaras invadían su intimidad, mostrando al mundo el interior de sus hogares, jardines y terrazas sin haberles pedido permiso. Google se ofreció inmediatamente a corregir aquellas invasiones accidentales de intimidad con un modesto pixelado. Era la coartada perfecta, porque la verdadera invasión estaba ocurriendo en la esfera de lo invisible: los coches iban capturando todas las señales wifi de todos los edificios por los que pasaban, incluyendo los nombres de las redes (ESSID), las IP, las direcciones MAC de los dispositivos. También se embolsaron la

gran cantidad de correos privados, contraseñas y todo tipo de transmisiones emitidas por redes abiertas y routers domésticos mal protegidos.

Cuando fueron descubiertos por las autoridades alemanas de protección de datos, Google declaró muchas cosas. La secuencia parece casi de comedia de situación. Primero dijo que en Estados Unidos era legal rastrear los paquetes de datos que flotaban en el espectro electromagnético porque es el espacio público y que otras empresas como Microsoft lo hacían de manera rutinaria. Después aseguró que la captura había sido un error causado por un código experimental que se había colado en el proyecto y que lo habían corregido de inmediato. Ya bordando el desaguisado, llegaron a decir que lo que habían cometido era una especie de servicio público, porque el «accidente» había demostrado a los ciudadanos lo vulnerables que eran las redes wifi abiertas y la importancia de proteger mejor la información. Pagaron siete millones de multa que, para Google, no es mucho. Si el plan era conectar las identidades digitales que tenían en sus bases de datos con las personas reales del mapa, incluyendo sus casas, sus coches y sus vecindarios, no les salió muy caro, pero podían haberse ahorrado ese dinero. Google ya no necesita husmear las calles para saber los nombres, direcciones, teléfonos y contraseñas de las personas cuyas casas y oficinas salen en los mapas. Para eso tiene Android, un sistema operativo que viene preinstalado en el 74,92 por ciento de los móviles de todo el mundo. Un dispositivo que el usuario mantiene encendido en todo momento, lleva encima a todas partes y tiene dos cámaras, un micrófono, una media de catorce sensores y al menos cuatro sistemas de geolocalización.

Cualquier espía te dirá lo mismo: el dato más valioso sobre una persona no son sus correos personales sino su posición geográfica. Sabiendo dónde está en cada momento de su vida sabremos dónde vive, dónde trabaja, cuántas horas duerme, cuándo sale a correr, con quién se relaciona, a dónde viaja, cómo se transporta de un sitio a otro, cuál es su terraza favorita. Frente qué escaparates se para, en qué tienda del mercado compra, si recicla, si se droga, si toma anticonceptivos o si va a la iglesia. Si va a conciertos al aire libre o prefiere los DJ, si come en restaurantes de comida rápida o es más bien gourmet. Sabemos quién le gusta y a quién intenta evitar, con quién come y cena, cuánto tiempo pasa con cada uno y a dónde va después. Sabemos si tiene un amante, si se hace el enfermo, si apuesta, si bebe. Sabemos cosas que la propia persona no sabe, como sus rutinas inconscientes y sus correlaciones sutiles. Un *smartphone* le cuenta todas esas cosas a las aplicaciones que lleva dentro, una mina de oro sin fondo para la industria de la atención.

OJOS EN EL BOLSILLO

Todos los teléfonos llevan un GPS (Global Positioning System) que se comunica con tres satélites que triangulan la señal para decir exactamente dónde están. Este sistema es independiente de internet, por eso podemos seguir viendo nuestro puntito en el mapa aunque no tengamos conexión o nos hayamos quedado sin datos. El GPS es un sistema estadounidense y, desde su lanzamiento en 1973, ha estado operado por las Fuerzas Armadas de Estados Unidos, que se reservan el derecho de alterar su precisión por motivos de seguridad. Pero su monopolio está a punto de acabar porque el mundo de los satélites está experimentando una silenciosa e importante revolución. Rusia tiene su propio sistema, llamado GLONASS; Europa está terminando Galileo con la Agencia Espacial Europea; China tiene Compass/BeiDou2 y Japón trabaja en el sistema Quasi-Zenith. Dan Coats, actual director de Inteligencia de Estados Unidos, declaró ante el Comité de Inteligencia del Senado que «Rusia y China sienten la necesidad de compensar cualquier ventaja que Estados Unidos pueda derivar de sus sistemas espaciales militares, civiles o comerciales y están considerando sistemas de ataque antisatélite como parte de su doctrina de guerras futuras». Ahora mismo todo el mundo quiere poner cosas en órbita. Según el Índice de Objetos Lanzados al Espacio Exterior, hay 4.921 satélites orbitando, incluido el descapotable rojo de Elon Musk.

El GPS no es el único sistema de geolocalización de un teléfono, hay al menos tres más. La tarjeta wifi tiene dos clases de sistemas de posicionamiento. El RSSI o indicador de intensidad de señal recibida mide la intensidad de la señal de un entorno de red inalámbrica y la compara con una base de datos de redes wifi para conectarse al más cercano. El algoritmo de posicionamiento más utilizado es Fingerprint y está basado en un mapa de conexiones anteriores (wifis a las que nos hemos conectado anteriormente). Después está el bluetooth, que emite señales de radio de corta frecuencia para conectarse a otros dispositivos sin usar un cable. Por ejemplo, la radio del coche, unos auriculares inalámbricos o un altavoz inteligente. Cuando está activado, busca dispositivos a los que conectarse dando información sobre el teléfono. Casi todos los dispositivos del internet de las cosas, de los altavoces a las básculas pasando por las muñecas parlantes, funcionan por bluetooth.

Si el móvil lleva una tarjeta SIM, está mandando constantemente una señal a las antenas de telefonía móvil más cercanas cada pocos segundos para recibir servicio. Las operadoras pueden calcular a qué distancia está el usuario de las distintas señales usando una tecnología llamada Cell ID. Cuanto más

densidad de antenas, mayor precisión. El rango máximo de una antena es de treinta y cinco kilómetros y registra todo lo que pasa en su dominio. A veces las autoridades piden a las operadoras la lista de todos los móviles que han pasado por las intermediaciones de una antena. Esta técnica se llama un volcado de torre (*cell tower dump*). El Gobierno ucraniano la usó en enero de 2014 para identificar a las personas que se manifestaban contra las últimas decisiones de su presidente Víktor Yanukóvich y mandarles un mensaje por SMS. Decía: «Querido usuario, ha sido registrado como participante en un disturbio masivo». También es utilizado por empresas de marketing para determinar las zonas de tránsito comercial para cadenas de ropa o restaurantes. Y por firmas como Securus Technologies, que venden servicios de motorización en tiempo real de teléfonos y llamadas para empresas, individuos e instituciones. En 2018, la empresa ofrecía un paquete especial para las prisiones de Estados Unidos, que al menos en un caso era utilizado por el director para vigilar a los funcionarios. La investigación posterior reveló que Securus compraba sus datos de una empresa de geolocalización llamada 3Cinteractive, que a su vez los compraba de LocationSmart, que los compraba directamente de las operadoras AT&T, Sprint, T-Mobile y Verizon. **[5]** Otra empresa llamada Microbilt vende el mismo servicio a empresas de seguros, vendedores de coches y otros negocios de venta a crédito para encontrar a los deudores. Otras empresas todavía más oscuras lo usan para localizar esposas supuestamente infieles, exmujeres y potenciales víctimas de violencia de género. «Le están vendiendo la información a la gente equivocada», declaraba un filtrador a Motherboard en 2019.**[6]** Una oscura industria de servicios que compra la misma clase de acceso que la policía o el FBI, sin orden judicial, registro o licencia.

Otra de las técnicas que usan las autoridades se basa en un dispositivo llamado StingRay o IMSI-catcher, que se hace pasar por una antena para rastrear todos los móviles que tiene alrededor.**[7]** Es como un «man-in-the-middle attack», una técnica que usan los hackers para interceptar información desprotegida interponiéndose entre un dispositivo y un router. La policía lo lleva en los helicópteros y furgonetas para determinar en tiempo real quién hay en una manifestación, o para encontrar a una persona dentro de un edificio o saber quién hay antes de entrar. Aunque usarlos es ilegal, un IMSR-catcher se puede fabricar con componentes legales por menos de cien euros. Hay foros que ofrecen maletines caseros de escucha por unos trescientos euros y equipos profesionales de policía por menos de dos mil.

Todas las aplicaciones que usan el GPS saben dónde estás en todo momento. Si hay cobertura, tu operadora también. La mayor parte de los servicios usan una combinación de las dos cosas para registrar las coordenadas con total precisión. Varios estudios realizados en 2017 demostraron que desactivar los servicios de localización de las plataformas digitales no impide que las compañías sigan localizando al usuario y usando esa información. Solo deja al usuario sin funcionalidades, como encontrar un lugar en Google Maps, conectar con personas cercanas en Tinder o especificar el lugar donde ha hecho la foto publicada en Instagram. Tanto Google como Facebook siguen registrando su posición y, por lo tanto, también las aplicaciones de su plataforma. Cuando no tienen acceso al GPS siguen geolocalizando el dispositivo gracias a la tarjeta wifi y la dirección IP. Una investigación del *New York Times* encontró docenas de empresas de marketing de localización extrayendo datos de hasta doscientos millones de móviles a partir de distintas aplicaciones en Estados Unidos, para después vender la información, analizarla para sus propios anunciantes o ambas cosas. **[8]** Los tres principales compradores son otras empresas tecnológicas, *data brokers* y consultoras políticas.

Hubo un tiempo en que la extracción se hacía con pleno conocimiento y hasta colaboración del usuario. En 2010, bautizado «el año de la localización», millones de usuarios de Foursquare anunciaban deliberadamente su llegada a cafés, restaurantes, festivales, centros comerciales, reuniones de empresa, museos, discotecas y hasta estaciones de tren con la intención de mantener informada a su agenda de contactos y producir conexiones «espontáneas». Muchos lo anunciaban a todo el mundo con actualizaciones automáticas en Twitter y Facebook. Cuando el año de la localización se convirtió en la década de la vigilancia, Foursquare perdió el favor de los usuarios y tanto ellos como el resto de las empresas prefieren extraer los mismos datos de manera más sutil, a través de otro tipo de aplicaciones. Entre 2009 y 2015, Twitter geolocalizaba cada tuit por defecto con precisas coordenadas GPS que no eran visibles para los usuarios ni para sus *followers* pero que sí para las aplicaciones de la API, y aparentemente permanecen visibles a día de hoy.**[9]** IBM compró las aplicaciones de Weather Channel que mucha gente usa en su pantalla de inicio para ver qué clima hace en la ciudad. Entre los grandes respaldos financieros del sector están gigantes de las finanzas como el grupo Goldman Sachs y contratistas militares como Peter Thiel, cofundador de PayPal y dueño de Palantir.

Además del geoposicionamiento, los *smartphones* tienen multitud de sensores. El giroscopio registra la posición y orientación del teléfono. Sabe cuándo estamos cogiendo el móvil con las manos para escribir en él y cuándo lo hemos puesto en horizontal para jugar, ver un vídeo o hacer una foto. Sabe si está en el bolso o en el bolsillo. El sensor lumínico indica si estamos con la luz encendida o apagada, y qué clase de luz es. El acelerómetro mide la velocidad y el sentido en el que nos movemos: es el que cuenta los pasos en las aplicaciones de *fitness* y sabe si vamos en coche o en bicicleta o en tren. También es fundamental para cazar Pokemon y otros juegos de realidad aumentada. El magnetómetro mide los campos magnéticos y aporta el compás a los mapas, pero también sirve como detector de metales. Algunos móviles como el iPhone tienen barómetros para detectar cambios de presión atmosférica y determinar la altitud. El frontal superior del móvil tiene un sensor de proximidad con dos leds de infrarrojos que le dice al sistema que el móvil está pegado a la oreja, para apagar la pantalla. A su lado, el sensor de luz ambiental mide la luz para calibrar el brillo de la pantalla. Los sensores son como los combos del Tekken: cuando usas cuatro a la vez son mucho más que la suma de sus partes. Un equipo de ingenieros de la Universidad de Newcastle demostró que solo con los datos de los sensores se pueden extraer hasta las contraseñas que teclea el usuario, tanto en las aplicaciones como en el navegador. «Hay programas maliciosos que pueden *escuchar* los datos de los sensores y revelar todo tipo de información delicada sobre ti —explicaba Maryam Mehrnezhad, miembro del laboratorio de Seguridad y Resistencia de Sistemas, del Departamento de Computación—, como tus llamadas, tus actividades físicas y todas tus interacciones táctiles, PIN y contraseñas. Y lo que es más preocupante: hay navegadores que, cuando abres una página —por ejemplo, la de tu banco— en un dispositivo que tenga instalado el software malicioso, puede espiar todos los datos que introduces». Según un estudio de la Universidad de Oxford, el 90 por ciento de las aplicaciones de Google Play —el kiosco de apps para teléfonos Android— comparte con Google los datos que recoge, a veces sin conocimiento de los desarrolladores. **[10]** La mitad de las aplicaciones comparte sus datos con diez terceras partes y hay un veinte por ciento de apps que los comparte con más de veinte. Esas terceras partes suelen incluir a Facebook, Twitter, Microsoft y Amazon. Casi todas vende los datos a uno o varios *data brokers*.

La cámara y el micrófono son los sensores más apreciados por los usuarios, y también los que más inquietud despiertan, con razón. Son los ojos y oídos del teléfono, y es imposible para el usuario saber cuándo están

funcionando y con quién se están comunicando. «De vez en cuando, los fragmentos de audio acaban en los servidores de una aplicación, pero no hay una explicación oficial de por qué pasa esto —contaba en 2018 el consultor de ciberseguridad Peter Hannay en *Vice Magazine*—.[11] No sabemos si sucede cada cierto tiempo o en ciertos lugares o para ciertas funciones, pero las aplicaciones están usando el micrófono y lo hacen de manera periódica». Tampoco podemos analizarlo sin la colaboración de las empresas implicadas, porque toda la información que envía la app está cifrada. Por otra parte, hay aplicaciones cuyo funcionamiento implica necesariamente un estado continuo de escucha, como los asistentes virtuales que vienen integrados en los últimos *smartphones*. Tanto el asistente de Google como sus competidores occidentales Siri (de Apple) y Alexa (de Amazon) activan sus funciones cuando alguien dice la palabra mágica: «O. K. Google», «Hey Siri» y «Alexa», respectivamente. Pero, para escuchar la palabra que los activa, tienen que estar escuchando en primer lugar. Amazon Echo, el «altavoz inteligente» de Amazon que funciona con Alexa, usa siete micrófonos para escuchar todo lo que ocurre a su alrededor. Eso no quiere decir que sea particularmente bueno separando la palabra mágica de cualquier otra.

En mayo de 2018, una mujer de Oregón se enteró de que su Amazon Echo había grabado una conversación privada que había mantenido con su marido y se la había enviado sin pedir permiso ni confirmación a un contacto de su agenda. No se enteró por la empresa, sino porque el contacto era alguien cercano a la familia que enseguida llamó para advertirles que habían sido «hackeados». La explicación de Amazon al *Washington Post* era digna de una comedia de enredo. Dijeron que el Echo había creído escuchar la palabra Alexa y se había activado, que la conversación que escuchó había sido interpretada como un mensaje que debía ser enviado y que, cuando preguntó a quién, «la conversación de fondo fue interpretada como un nombre de la lista de contactos del usuario». Un usuario alemán que usó la regulación de protección de datos europea para solicitar a Amazon todos los datos que tuviera sobre él, recibió mil setecientos archivos de audio de otra persona. Amazon declaró que se trataba de un «desafortunado caso de error humano y un accidente aislado». Además de venir instalados por defecto en los dispositivos de sus respectivas empresas, como los iPhones y los Android y los Echo y los Dots, los gigantes pelean ahora por colonizar con sus algoritmos el resto de consolas, vehículos, televisores, webcams, lámparas, tablets, electrodomésticos y hasta aplicaciones «inteligentes» de otras marcas. El de Google está integrado en videocámaras domésticas de Nest, pantallas de

Lenovo, despertadores como iHome, televisores de Philips, altavoces de Onkyo, LG, Klipsch, Braven y JBL y hasta en el asistente de estilo del gigante japonés Uniqlo, que utiliza la tecnología de Mountain View. Alexa viene por defecto en al menos ciento cincuenta productos diferentes, incluyendo estrellas del mercado como la barra-altavoz de Sonos Beam y los microondas de Whirlpool. Naturalmente, Tesla tiene su propio asistente para sus coches. Pronto será imposible comprar tecnologías que no escuchen lo que hacemos en nuestra casa, vehículo, oficina, todo lo que ocurre a su alrededor y envíen toda clase de datos a las mismas cinco compañías, sin que podamos saber para qué los usan ni durante cuánto tiempo ni con quién más. Como no tenemos acceso a su código, tenemos que buscar en los lugares donde se manifiestan sus objetivos, como la oficina de patentes. Google ha presentado patentes para determinar el estado mental y físico del usuario usando datos del micrófono, como el volumen de la voz, el ritmo de la respiración o el sonido de llanto. Amazon ha patentado un algoritmo que analiza la voz en tiempo real, buscando palabras y expresiones que indiquen preferencia, interés o rechazo por cualquier cosa que se pueda transformar en productos o servicios. Son los planes de un modelo publicitario basado en una intrusión extrema y una manipulación sutil, del que hablaremos más adelante. Aquí lo importante es el reconocimiento de un conjunto de dispositivos de escucha extremadamente sofisticados en permanente estado de alerta que nos acompañan a todas partes.

Los *smartphones* tienen al menos dos cámaras, una por delante y otra por detrás. Las aplicaciones que tienen acceso a la cámara pueden encender y apagar cualquiera de las cámaras sin permiso, y hacer fotos y vídeos sin permiso, mandarlos a un servidor sin permiso y hacer retransmisiones en *streaming*.**[12]** También pueden enviar fotos y vídeos de un rostro al servidor para que un algoritmo de reconocimiento facial los compare con otros de una base de datos, o para crear un modelo 3D de ese rostro para una base de datos de reconocimiento facial. También puede hacer fotos de las yemas de los dedos que tocan la pantalla. Naturalmente, todas estas funciones están aseguradas si usamos nuestra cara, nuestra huella dactilar o nuestra voz para desbloquear el teléfono. Todas las aplicaciones de identificación biométrica recogen, analizan y almacenan nuestros datos biométricos. Son los datos más protegidos por las leyes de protección de datos porque, a diferencia de una clave o de un número de teléfono, no se pueden cambiar. Nos hacen reconocibles para el resto de nuestra vida. Por lo menos en el mundo real.

En 2014, Google compró una empresa británica de inteligencia artificial llamada DeepMind por quinientos veinte millones de dólares. Su logro más notable fue pulverizar en una partida de Go, un juego supuestamente improgramable, al mejor jugador del mundo. El más preocupante fue usar los datos de millones de usuarios de la Seguridad Social británica sin el permiso de los propios pacientes con el fin de desarrollar algoritmos de detección de enfermedades para Google. Es importante entender que toda esa información acaba en el mismo sitio y que es usada de la misma manera para cosas distintas: el algoritmo capaz de identificar los síntomas de un enfisema es el mismo que opera los sensores de la mayor parte de los móviles que hay en el mercado, y que usará el llanto, el pulso y la respiración del usuario para determinar su estado de salud. Y es el mismo que procesa las diez mil millones de preguntas diarias que responde el buscador, incluyendo consultas íntimas sobre enfermedades y condiciones mentales. La tercera pregunta más popular de 2018 fue sobre endometriosis. Aparentemente, es la enfermedad que afecta al tejido del útero de Lena Dunham, autora de la serie *Girls*. La cuarta fue cuánto tiempo permanece la marihuana en la orina. La quinta: cuándo me voy a morir.

«Una de las cosas que acaba pasando es que ya no necesitas teclear nada —presumía Eric Schmidt en 2010—. Porque sabemos dónde estás. Sabemos dónde has estado. Podemos adivinar más o menos lo que estás pensando». Después declara que «un día comentamos que podríamos predecir los mercados y decidimos que era ilegal. Así que dejamos de hacerlo». Pero no dejaron de hacerlo. En 2015, Google pasó a ser subsidiaria de Alphabet Inc. junto con otras ocho empresas, incluidas dos divisiones financieras; CapitalG (fondo de capital de riesgo) y GV (inversión de capital riesgo); dos laboratorios de investigación médica, Calico (biotecnológica para la longevidad) y Verily (investigación genética y de enfermedades); tres de infraestructura de cable (Google Fiber); sensores (Nest) y Smart Cities (Sidewalk Labs). Y finalmente, su laboratorio de investigación y desarrollo secretos, llamada Google X. En realidad todas son secretas. Y todas hacen lo que hacía Google; ofrecer servicios a cambio de datos a usuarios cada vez más críticos: bancos, hospitales, administraciones, sistemas de transporte, fábricas, colegios.

Después de Snowden

La primera filtración de Edward Snowden que se publicó en la prensa era sobre llamadas. En abril de 2013, el *Guardian* publicó que «la Agencia de Seguridad Nacional (NSA) está registrando las llamadas telefónicas de millones de ciudadanos estadounidenses usuarios de Verizon». Verizon fue el monstruo que surgió de la liberalización de 1996. Era hija de Bell Atlantic Corp. y GTE Corp., la fusión más grande de la historia de Estados Unidos. También era nieta de AT&T. En 1984, el Gobierno había obligado a trocear la compañía para acabar con el monopolio y Bell Atlantic era una de las siete hijas regionales, llamadas «Baby Bells». Cuando, en abril de 2008, el FBI logró que el Tribunal de Vigilancia de Inteligencia Extranjera obligara a Verizon a entregar sus registros a la NSA, consiguió de golpe acceso a prácticamente todas las llamadas telefónicas realizadas en Estados Unidos. La centralización es un imán para la vigilancia. También tenía los datos de localización de todos sus clientes, con nombre, apellido y cuenta bancaria.

La segunda entrega del archivo Snowden, dos días más tarde, documentaba un proyecto llamado PRISMA con el que el Gobierno de Estados Unidos mantenía un acceso directo a los servidores de las principales empresas tecnológicas, incluidas Google, Facebook, Apple, Amazon y Microsoft desde al menos 2008, y que compartía su acceso con otros países de la llamada Alianza de los Cinco Ojos: Inglaterra, Australia, Nueva Zelanda y Canadá. El programa había sido legalizado por el Gobierno de Barak Obama gracias a un entramado complejo de tribunales secretos y leyes antiterrorismo. La sección 702 de la Ley de Vigilancia de la Inteligencia Extranjera (FISA) concedía a la NSA el acceso a todas las comunicaciones privadas que trascendieran las fronteras estadounidenses. La sección 215 de la USA-Patriot Act autorizaba la intromisión del Gobierno en los registros que están en manos de terceras partes, incluidas cuentas bancarias, bibliotecas, agencias de viaje, alquileres de vídeos, teléfonos, datos médicos, de iglesias, sinagogas, mezquitas y, naturalmente, plataformas digitales. Todo esto ocurría con la autorización de un tribunal secreto, diseñado para los asuntos secretos, y sin el conocimiento o el consentimiento de las personas espiadas. La Patriot Act también prohibía expresamente que las empresas registradas informaran a sus propios usuarios de que sus datos habían sido comprometidos.

En su primera intervención pos-Snowden, el presidente Barack Obama quiso tranquilizar a sus constituyentes asegurando que la ley no permitía a las agencias leer el contenido de las comunicaciones sino solo registrar los metadatos, una información pública que no requería una orden judicial para

ser interceptada. Como jefe de las Fuerzas Armadas, tenía que saber que eso no es verdad. El consejero general de la NSA, Stewart Baker, confesó que «los metadatos te cuentan absolutamente todo acerca de la vida de alguien. Si tienes suficientes metadatos no necesitas contenido». «Nosotros matamos gente usando metadatos», declaró el general Michael Hayden en un debate titulado *Re-evaluando la NSA*.[13] Si tienes suficientes, los metadatos te cuentan cosas que el vigilado no sabe. En la era del Big Data, el contenido es lo menos valioso. El metadato es el rey.

El director nacional de Inteligencia, James Clapper, defendió públicamente el proyecto PRISMA como una fuente crucial de inteligencia antiterrorista. «La información que hemos conseguido a través de este programa es inteligencia de la más alta importancia y valor». Era el mismo director que, tres meses antes, juró ante el comité de Inteligencia del Senado que la NSA no recopilaba ni almacenaba datos de millones o cientos de millones de estadounidenses. El resto de protagonistas negaron fríamente su colaboración. «Nosotros facilitamos datos de usuarios al Gobierno de acuerdo con la ley, y revisamos los casos cuidadosamente —decía el comunicado de Google—. […] Google no tiene una puerta de atrás por la que el Gobierno accede a los datos privados de los usuarios». Un portavoz de Apple dijo que nunca había oído hablar del proyecto PRISMA, contradiciendo directamente los documentos oficiales comprobados y publicados por los principales medios del país. Mintieron como mintió el jefe de Inteligencia Nacional al órgano constitucional de su propio Gobierno. En estas circunstancias, no tiene sentido preguntarse, desde la sociedad civil, si estas empresas y sus ejecutivos son moralmente capaces de ejercer la censura, coartar las libertades civiles o traicionar la confianza de los usuarios. Como sabían los arquitectos del TCP/IP, todos los debates sobre la bondad o la maldad de las empresas son una distracción. Los directivos cambian o son despedidos o mienten o están sujetos a legislaciones y a gobiernos que cambian o mienten. La única pregunta relevante en el debate es si desarrollan tecnologías capaces de ejercer la censura, coartar las libertades civiles o traicionar la confianza de los usuarios. Si lo hacen, es siempre un problema independientemente de su intención.

Los papeles de Edward Snowden eran escandalosos porque demostraban que los ciudadanos estadounidenses habían sido espiados por su propio Gobierno en su propia casa, vulnerando derechos fundamentales protegidos por la Constitución. El aparato de espionaje gubernamental había sido usado anteriormente para desprestigiar movimientos civiles a través de sus líderes.

Durante su reinado como director del FBI, J. Edgar Hoover mantuvo un fuerte aparato de espionaje alrededor de Martin Luther King, especialmente después de que les acusara de ser «completamente ineficaces en la resolución de la continua violencia y brutalidad infligida sobre la comunidad negra en el sur profundo». El programa de contrainteligencia acumuló un dosier donde se le acusaba de mantener relaciones ilícitas con al menos cuatro mujeres (entre ellas la cantautora Joan Baez) y de participar en orgías con alcohol y prostitutas (negras y blancas). También se le acusaba de tener lazos con el Partido Comunista y de evadir impuestos para su organización. Entonces el presidente era Lyndon B. Johnson, que ocupaba el cargo en sustitución de John F. Kennedy, asesinado en 1963. Hoy el presidente es Donald Trump. En el momento de escribir estas líneas, el presidente mantiene secuestradas todas las funciones del Gobierno hasta que el Congreso apruebe una partida de cinco mil millones de dólares para construir un muro en la frontera con México. «Si no conseguimos lo que queremos, cerraré el Gobierno», les dijo a la presidenta de la Cámara del Congreso Nancy Pelosi y al líder de la minoría demócrata Chuck Schumer, el 2 de diciembre de 2018. A finales de enero, todos los trabajadores cuyas nóminas dependen del Estado, desde los funcionarios de las administraciones hasta los barrenderos, siguen sin cobrar. Todas las instituciones que dependen de las partidas del Gobierno, como los juzgados, los servicios sociales o los parques nacionales se están viniendo abajo. La máquina de espionaje más grande de la historia está en manos de un líder deshonesto, rencoroso y vengativo. Numerosos informes oficiales afirman que Donald Trump ocupa el puesto gracias al abuso coordinado del aparato de vigilancia y la manipulación comercial de las plataformas digitales. Es poco probable que use el poder con más responsabilidad que el resto.

Snowden había denunciado el abuso de poder en suelo estadounidense, pero los ciudadanos del resto del mundo son espiados legalmente por las agencias de inteligencia de Estados Unidos. No tenemos derechos civiles en suelo americano, nuestros datos son barra libre para cualquier agencia de inteligencia exterior. Con una excepción. La Cámara de Comercio de Estados Unidos tenía un pacto de caballeros con la Unión Europea. La Directiva europea sobre protección de datos de 1995 estaba diseñada para proteger a los ciudadanos europeos de las empresas que solicitan datos para ofrecer servicio a los clientes, como las compañías telefónicas, los bancos, servicios de transporte, proveedores de gas, electricidad, agua, etcétera. Todas las compañías europeas entraban la directiva y, por lo tanto, había libre circulación de datos entre compañías europeas. Pero quedaba prohibida la

exportación de datos a jurisdicciones de fuera de Europa, como Estados Unidos. Con la globalización y la llegada de internet, millones de europeos empezaron a usar servicios y plataformas de comunicación estadounidenses: correos de Yahoo y Gmail, cuentas en Facebook, MySpace, Twitter, aplicaciones para móvil como WhatsApp, 4Square, etcétera. Todas esas cuentas de usuario quedaban almacenabas en servidores y bases de datos fuera de Europa. En el año 2000, la Comisión Europea firmó una excepción desarrollada por el Departamento de Comercio de Estados Unidos, según la cual las empresas se comprometían a mantener los principios de la Directiva 95/46/CE para todos los datos procedentes de Europa, llamado Safe Harbour (puerto seguro). Pero no estableció los medios para asegurar que las empresas cumplían el pacto. Y las empresas no lo hacían, como descubrió un joven austriaco llamado Max Schrems.

Schrems estaba cursando un semestre de Derecho en la Universidad de Santa Clara en Silicon Valley, cuando uno de sus profesores trajo a Ed Palmieri, el abogado de Facebook especializado en privacidad, para que diera una charla en clase. A Max le sorprendió lo poco que sabía sobre legislación europea en materia de protección de datos, y decidió que su trabajo para aquella clase sería una investigación sobre Facebook en el contexto de las directivas europeas. Mientras investigaba, descubrió que Facebook no solo acumulaba enormes dosieres de sus usuarios sino que cruzaban el Atlántico sin respetar el tratado de Safe Harbour. Como casi todos los gigantes tecnológicos, Facebook tenía su sede europea en Irlanda. «Eso significa que todos sus usuarios europeos tienen un contrato con la oficina de Dublín, lo que les hace sujetos de la ley de protección de datos en Irlanda», explicó Schrems.**[14]** Uno de esos derechos era el de saber qué datos tiene una compañía sobre ellos.

Schrems encontró la página para solicitar los datos enterrada en lo más profundo de la web de Facebook. Cursó su solicitud y recibió un CD con un documento de mil doscientas páginas. Allí encontró un dosier con todas las veces que se había logueado, desde dónde, durante cuánto tiempo y con qué ordenador. Qué otras personas se habían logueado alguna vez desde los mismos sitios. Todas las personas que había marcado como amigos y también las que había desmarcado, con la fecha y duración de todas ellas. Todas las direcciones de correos de sus amigos; todas las personas a las que había «pokeado» y todos los mensajes y chats que había escrito, incluyendo los que había borrado después. Todas las fotos que había visto, todas las cosas que había leído, todos los enlaces que había pinchado. Max no era una persona

conocida ni relevante para la empresa. El registro era automático, parte del algoritmo. Eso significaba que todos y cada uno de los usuarios de Facebook tenían un «dosier» similar. Y que la falta de supervisión era extensible a todas las compañías extranjeras que guardaban datos de ciudadanos europeos, incluyendo Google, Apple, Twitter, Dropbox, Amazon y Microsoft.

Schrems creó una página llamada europe-v-facebook donde iba publicando su investigación. Cuando publicó su dosier, los medios recogieron la noticia y cientos de personas le pidieron a Facebook sus datos. Cuando llegó a Reddit, muchos estadounidenses descubrieron que no tenían derecho a solicitarlos. Europa tenía ley de protección de datos, Estados Unidos no. Ser europeo tampoco era suficiente. A pesar de las múltiples demandas que abrió Schrems en Irlanda, Facebook se negó a entregarle los datos biométricos (derivados de su cara), argumentando que la tecnología utilizada para generarlos era un secreto industrial. «Yo no soy más que un tío normal que ha estado en Facebook durante tres años —escribió Schrems—. Imagínate esto dentro de diez años: cada manifestación a la que he ido, mis tendencias políticas, mis conversaciones íntimas, mis enfermedades». Cuando el *Guardian* publicó los documentos del proyecto PRISMA, Schrems ya no tuvo que demostrar que Facebook espiaba a sus usuarios europeos, incumpliendo el acuerdo de Safe Harbour. Llevó el caso al Tribunal de Justicia europeo con los papeles de Snowden y lo ganó. El acuerdo de transferencia de datos entre la Unión Europea y Estados Unidos fue anulado. Cinco meses más tarde, la Comisión presentó un nuevo acuerdo transatlántico para el intercambio comercial de datos personales llamado Privacy Shield (escudo de privacidad). «La NSA guarda un registro de todo lo que hace un ciudadano europeo, independientemente de si hace algo malo o no —me dijo Edward Snowden en 2016—. Y pueden acceder a ese registro sin una orden y examinar todos los archivos. La única diferencia es cómo los tratan después de haberlos investigado». Facebook tenía entonces un total de 845 millones de usuarios. Tres años más tarde tiene 2.220 millones, sin contar los de otras dos empresas que también son suyas, Instagram y WhatsApp.

La estrecha relación de las plataformas con la administración no se limita al Gobierno estadounidense. Los contratos gubernamentales son los más golosos, incluso si son gobiernos autoritarios en franca oposición a los supuestos valores de la empresa. En 2018, cuatro mil empleados de Alphabet firmaron una petición en Medium para que abandonara el proyecto Dragonfly, un buscador censurado con una lista negra de páginas sobre derechos humanos, democracia, religión, activismo, vigilancia y otros contenidos

indeseables para el Gobierno chino. «Muchos de nosotros aceptamos trabajar para Google con los valores de la compañía en mente, incluida su anterior postura con respecto a la censura y la vigilancia chinas, y dando por hecho que Google era una compañía dispuesta a poner sus valores por encima de sus beneficios». Unos meses más tarde, tres mil cien empleados publicaron en el *New York Times* una carta para el presidente ejecutivo de Google, Sundar Pichai. Querían que abandonara el desarrollo de inteligencia artificial para mejorar el proceso de vídeo y la orientación de los ataques de los drones del ejército estadounidense. «Creemos que Google no debería estar en el negocio de la guerra», empieza la carta. Pero Google es parte del negocio de la guerra, como todas las grandes tecnológicas estadounidenses. Eric Schmidt es consejero del Departamento de Defensa, Vint Cerf fue contratado como «evangelista jefe» de Google, embajador perfecto entre la empresa y el Pentágono. En 2004, Google hizo un buscador especial para la CIA en el que escanearon todos los archivos de Inteligencia. Pidieron cambiar una de las O del logo por el sello de la agencia y Google puso una condición. «Le dije a nuestro departamento de ventas que les dieran el ok si prometían no contárselo a nadie —contaba Douglas Edwards en su libro de memorias *I'm feeling lucky*—. No quería espantar a los activistas de la privacidad». En 2007 trabajaron con Lockheed Martin, empresa clave del complejo industrial-militar estadounidense, para desarrollar un sistema de inteligencia visual para la Agencia de Inteligencia Geoespacial con las bases militares que tenían en Irak y Afganistán. El sistema señalaba los barrios de población chiita y sunita que estaban siendo rápidamente diezmados en una campaña de limpieza étnica. Era la clase de proyecto para el que se había creado Google Earth. Cuando el huracán Katrina arrasó el Golfo de México, Google asistió a los helicópteros de rescate y la guardia costera localizando víctimas superponiendo a su imagen habitual del globo terráqueo una capa actualizada en tiempo real, procedente de sus proveedores habituales, el Instituto Nacional Oceánico y Atmosférico y el operador civil de teledetección espacial DigitalGlobe. En 2010 recibió un contrato sin concurso de veintisiete millones de dólares para desarrollar el nuevo Servicio de Visualización GEOINT (GVS) para proporcionar visión del globo en tiempo real a soldados estadounidenses con capas de datos clasificados. «GVS fue construido para proporcionar una versión de Google Earth para las capas clasificadas secreto y alto secreto para visualizar información clasificada de manera geoespacial y temporal en una imagen compartida por la operación», explicaba el coronel Mike Russell de las Fuerzas Armadas. La tecnología está integrada en los

visores de Comandos de Combate de Defensa, pero también es utilizada por el FBI, CIA, NRO, NSA y la Agencia Federal de Gestión de Emergencias. Irónicamente, su actuación en momentos de crisis nos abre una ventana a su rango de habilidades.

Centinelas celestes

Los sistemas de imagen por satélite son parte de un circuito cerrado de vigilancia a nivel planetario en manos de un puñado de empresas que trabajan para distintos gobiernos. Sus grandes ojos rotantes no solo vigilan lo que ocurre dentro de sus fronteras. Registran todo lo que pasa en la superficie terrestre, incluyendo océanos, producción agrícola y ganadera, extracción de crudo y minerales, infraestructuras, ciudades, fábricas, transportes, refugios, personas. Cada minuto del planeta es localizable en el espacio y en el tiempo. Y accesible con la ayuda de un buscador.

Es el buscador de Google, pero en lugar de «organizar la información del mundo y hacerla accesible y útil para todos los usuarios», lo que hace es organizar la información del planeta y hacerla accesible y útil para sus clientes y asociados. Mucha gente piensa que esos datos se usan principalmente para predecir el tiempo o detectar fuegos e inundaciones. En verdad, lo que hacen las empresas de análisis por satélite es contar. Cuentan los coches en los aparcamientos, un servicio que usan al menos doscientos cincuenta mil garajes de Estados Unidos para informar a los supermercados y centros comerciales circundantes de la esperanza de venta que tienen cada minuto del día. También cuentan la cantidad de paneles solares que se instalan en cada región o los barriles de crudo que circulan en el mercado. La firma de análisis geoespacial Orbital Insight se chiva regularmente de que China tiene mucho más petróleo del que dice tener, y que está acumulando reservas a velocidad preocupante. Según James Crawford, presidente ejecutivo de Orbital, «representa la capacidad de China de aprovecharse de cualquier alteración de precio en el mercado».

Las empresas compran información satelital para calcular cuántas toneladas de cereal, legumbre o grano se van a recoger esta temporada, o cuántas cabezas de ganado tiene cada uno. «Lo genial de estas técnicas es que tradicionalmente tenías que hablar con un montón de granjeros para conseguir un estimado como el del Departamento de Agricultura —explicaba Mark Johnson, jefe de la *start-up* de predicción por satélite Descartes Lab en *The Verge*—. Con *machine learning* nosotros miramos todos esos píxeles de los

satélites y nos cuenta lo que está creciendo». Sus predicciones son mejores que las del Departamento de Agricultura porque el Gobierno puede saber lo que han sembrado, no necesariamente lo que van a recoger. Los satélites vigilan la cosecha minuto a minuto y tienen visión espectral para medir, entre otras cosas, los niveles de clorofila. Saben lo que está plantando cualquier agricultor y pueden sumar ese dato al resto de los datos de todas las cosechas en Brasil, Argentina, China, el Mar Negro y la Unión Europea. Tienen datos oficiales para compararlos con un siglo de cosechas anteriores y contrastarlos con las predicciones meteorológicas y otras mediciones relevantes sobre el estado de la tierra (minerales, humedad, población de insectos, contaminación de las áreas circundantes) para predecir el comportamiento del mercado. Los agricultores independientes no pueden negarse a facilitar los datos sobre lo que sucede en su propia finca, porque están vigilados desde lo alto por el ojo sin párpados de máquinas calculadoras e impertérritas. Pero las empresas que registran toda esa información puede ocultar sus algoritmos, sus objetivos y hasta su lista de clientes porque «la gente que vende suministros al negocio agrícola es muy celosa de sus fuentes de información».[15] Crawford trabajó para el proyecto de Google en la NASA, antes de fundar Orbital Insight en 2013.

La Unión Europea usa satélites para controlar el uso que hacen los agricultores de las ayudas directas de la Política Agrícola Común (PAC). Por ejemplo, vigilan que los agricultores cumplan con las medidas establecidas, como la rotación de cultivos, el mantenimiento de terrazas y que no labren las tierras a favor de la pendiente. El Ministerio de Agricultura español los usa para hacer previsión meteorológica, evaluar daños, monitorizar ayudas y hacer sus mapas detallados de cultivos y aprovechamientos de España. La verdad es que no se puede plantar un alcornoque sin que lo sepa el Estado, tanto si recibes ayuda como si no. Es un hecho históricamente aceptado que la agricultura es el principio fundacional de las naciones-estado, y que nuestra afición por el grano está más vinculada a la recaudación y el control de las cosechas que a la facilidad intrínseca de la semilla o a nuestra natural inclinación hacia ella. Los últimos estudios osteológicos insinúan que los *Homo sapiens* que dependían del grano eran más enclenques y estaban peor alimentados que los cazadores nómadas, y que enfermaban con más frecuencia. Pero tenían más hijos y estaban más respaldados por la comunidad, lo que facilitó su supervivencia. En su fascinante ensayo *Against the grain*, James C. Scott establece la elección del grano como fuente principal de alimentación por ser un material fácilmente tasable por el

Gobierno central. El campesino no puede ocultar una cosecha que crece por encima del suelo, y que necesita ser recogida y procesada en momentos específicos del año. Las comunidades donde plantaban patatas, boniatos y otros tubérculos que crecen bajo la tierra y pueden ser recolectados por tramos, según necesidad, ofrecían menos facilidades.

Vigilar el grano es vigilar al jornalero. Scott establece el ritual de la cosecha como el principio del largo y contestado proceso de automatización del hombre por el hombre. Una rutina de ejecución primigenia y extraordinariamente larga:

> La domesticación de las plantas quedó representada finalmente como la plantación de un terreno fijo […] que nos atrapa en un conjunto de rutinas anuales que organizan nuestra vida laboral, nuestros patrones de asentamiento, nuestras estructuras sociales. […] La cosecha misma establece otro paquete de rutinas: en el caso de los cereales hay que cortar, empacar, trillar, espigar, separar la paja del grano, tamizar, secar, sortear… gran parte de ese trabajo quedó establecido como funciones femeninas. En el momento en que los *Homo sapiens* tomamos la decisión fatal de meternos en agricultura, nuestra especie se encerró en el austero monasterio cuyo trabajo consiste fundamentalmente en el exigente horario genético de un puñado de plantas.

En un mundo dominado por los datos del satélite, no es difícil imaginar cierto favoritismo por cosechas favorables a la tecnología. «Los campos de maíz son muy buenos para la resolución de los satélites —dice Johnson— porque son grandes, el maíz crece despacio y no se mueve».

Los granos y el ganado son contables. Las personas, también. DigitalGlobe tiene un proyecto colectivo para contar las focas que quedan en el mar de Weddell en la Antártida pero también ayuda a Facebook a localizar a miles de millones de personas desconectadas de la red. Los satélites están equipados con diferentes tecnologías y radares, especialmente para distinguir objetos pequeños en grandes extensiones de agua. MarineTraffic es el servicio online más popular de seguimiento de barcos, pero usa el Sistema de Identificación Automática (AIS) por el cual el satélite manda un «ping» al barco y este devuelve su posición. No todos los barcos responden. El barco que pesca ilegalmente en el mar del Sur de China o transporta personas de forma clandestina se suele dejar el transmisor en casa, pero es imposible que se esconda del espacio. Hasta la barca más raquítica es localizable desde radares satélite como el VIIRS (Visible Infrared Imaging Radiometer Suite) de Raytheon, uno de los contratistas de defensa militares más grandes de Estados Unidos, que detecta luces en el agua. O por el sistema SAR (Synthetic Aperture Radar), que detecta cualquier trozo de metal que tenga más de seis metros de largo.

SpaceKnow hace índices económicos basados en una combinación de datos satelitales. Durante la primavera de 2018 estuvo vigilando la actividad de seis mil plantas industriales en China para evaluar su producción. El vicepresidente Hugh Norton-Smith dice que su plan es indexar el desestructurado y caótico mundo físico en una plataforma digital en tiempo real. En el contexto de la crisis climática, la soberanía de las infraestructuras de control y gestión de recursos valiosos como el grano, la ganadería o el agua es tan crucial como la capacidad de trazar el movimiento de las personas. Los satélites son solo una parte de esa gran infraestructura, además de un elemento crucial en el entramado de supervigilancia que los consorcios han bautizado como 5G. En 2015, la Agencia Geoespacial movió GVA a la nube de Amazon, AWS.

EL ESTADO SOBERANO DE LA NUBE

Amazon tiene la mitad del negocio mundial de la nube. Es el negocio más lucrativo y poderoso de Jeff Bezos, aunque mucha gente piense que se ha convertido en el hombre más rico del planeta regentando una tienda de libros online. De todos los gigantes tecnológicos, Amazon ha sido sin duda el más discreto. No tiene eslogan ni lema, no dice que vaya a hacer del mundo un lugar mejor o mejor conectado. Pero en sus servidores está alojado más de un tercio de internet. Claro que Amazon ofrece mucho más que alojamiento. AWS vende servicios de software e infraestructura que permiten a cualquier empresa ofrecer un servicio de vanguardia a sus clientes con la mayor seguridad, sin tener que comprar su propia tecnología. Netflix usa AWS para asegurarse de que sus contenidos llegan en perfecto *streaming* a todos los rincones y dispositivos del planeta, Unilever para sostener mil setecientas tiendas online, WeTransfer para sostener los envíos de grandes paquetes de datos, imperios mediáticos como Guardian News & Media o Hearst Corporation para sostener sus cabeceras web, Ticketmaster para vender entradas, el Centro Internacional de Investigación de Radioastronomía para mantener un espacio colaborativo donde se intercambian cantidades literalmente astronómicas de datos. También lo hacen Dow Jones y el NASDAQ, las plataformas Airbnb, Slack, Pinterest, Coursera, Soundcloud, The Weather Company y el Laboratorio de Propulsión de la NASA. Incluso el servicio de mensajería encriptada Signal, recomendado por Snowden y utilizado por activistas de la privacidad en todo el mundo. El poder horizontal de Amazon se expande por la industria de servicios ofreciendo un acceso

ilimitado a los datos que generan. Su vigilante dominio no solo afecta a los usuarios de cada una de esas aplicaciones sino también a las empresas mismas, porque Amazon puede estudiar sus modelos de negocio como si fueran ensayos de laboratorio para después destruirlos con precios imbatibles. AWS es la reina inconquistable del negocio, pero no está sola. Le siguen —a creciente distancia— Microsoft Azure, Google Cloud e IBM Cloud. Su único competidor real es Alibaba, que domina el continente asiático y en los últimos dos años ha empezado una agresiva expansión. Si internet se rompe en varios bloques, como ha sugerido el fundador de Google, estas dos nubes serán dos de los continentes principales.

Desde un punto de vista materialista, ya son reinos autogestionados con las necesidades de un país mediano. Contra lo que su vaporoso nombre sugiere, la nube es una aglomeración de silicio, cables y metales pesados que se concentra en lugares muy concretos y consume un porcentaje alarmante de electricidad. En 2008 ya producía el 2 por ciento de las emisiones globales de CO_2, y se espera que en 2020 haya duplicado esa marca, si no ha ocurrido ya. Dicen que una de sus principales causas es la «contaminación durmiente». Cada día se generan 2,5 quintillones de datos, en parte enviando colectivamente 187 millones de correos y medio millón de tuits, viendo 266.000 horas de Netflix, haciendo 3,7 millones de búsquedas en Google o descartando 1,1 millones de caras en Tinder. Pero muchos de los datos son generados involuntariamente por personas desprevenidas cuyas acciones y movimientos son registrados minuciosamente por cámaras, micrófonos y sensores sin que se den cuenta. Unos y otros se acumulan por triplicado en servidores de una industria que no borra nada, y que requiere refrigeración constante para no sobrecalentar los equipos. Cisco calcula que en 2021 el volumen aumentará en un 75 por ciento, cuando el internet de las cosas y las Smart Cities hayan puesto todos los objetos en red.

Tanto Google como Apple aseguran que sus centros funcionan con energías renovables desde 2017; Microsoft y Amazon dicen que avanzan en la misma dirección. Pero es difícil comprobarlo, especialmente en países donde no funciona la ley de transparencia. La realidad es que la nube se ha ido concentrando en lugares donde la electricidad es barata y la administración es generosa con las rebajas fiscales, la disponibilidad de mano de obra barata y la ausencia de protección de datos. Según Arman Shehabi, investigador del Laboratorio Nacional Berkeley, solo los servidores de iCloud y Google usan el 1,8 por ciento del consumo total en Estados Unidos. Un estudio de Japón, el segundo país más grande en consumo de Amazon, advierte que en 2030 la

red habrá superado todos sus recursos energéticos. En el futuro, los japoneses tendrán que elegir entre el aire acondicionado y la mensajería instantánea, entre la lamparita de noche y la retroiluminación del teclado. Capítulo aparte merecen los centros de datos dedicados a Bitcoin. Dos investigadores de la Oficina de Investigación y Desarrollo de la Agencia de Protección Ambiental de Estados Unidos calcularon que entre 2016 y 2018, solo la «extracción» produjo entre tres y trece millones de toneladas de dióxido de carbono, el equivalente al producido por un millón de coches.[16] En diciembre de 2018, varios departamentos financieros anunciaron que el precio de minar bitcoin había superado el valor de la propia divisa. «Ahora mismo, los únicos lugares donde aún da beneficios son China e Islandia —contaba el director de estrategia de Meraglim, James Rickards, en el *New York Post*—. Los dos tienen electricidad muy barata e Islandia tiene la ventaja de las bajas temperaturas para enfriar los ordenadores».

La nube devora recursos valiosos en tiempos de escasez, pero las ciudades se pelean por ella. Según los sociólogos David Logan y Harvey Molotch, el extraño fenómeno responde a un modelo de ciudad como «máquina de crecimiento», en el que las administraciones ofrecen incentivos a la industria que teóricamente fomentan el crecimiento económico aunque tenga que sacrificar recursos locales y empeore el nivel de vida de los sectores más vulnerables de la población.[17] El condado en el que se encuentra Tysons Corner, Virginia, donde el gran nudo de internet ha generado la mayor concentración de nubes del mundo, se ha convertido en el más rico de Estados Unidos, con una renta media anual de 134.464 dólares por hogar. «Este año […] vamos a tener 250 millones de dólares en ingresos tributarios solo de los centros de datos», presumía el jefe de desarrollo económico del condado, Buddy Rizer. Amazon Web Services llegó allí en 2006 y opera ahora en treinta y ocho plantas. También tiene ocho centros en San Francisco, ocho en Seattle y siete al noroeste de Oregón. En Europa tiene siete en Dublín, cuatro en Alemania, tres en Luxemburgo. En el Pacífico tiene doce centros en Japón, nueve en China, seis en Singapur y ocho en Australia. En Latinoamérica solo tiene seis centros, y están en Brasil. La nube solitaria más hambrienta y voluminosa es la que mantiene la NSA en el desierto de Utah, la primera capaz de contener un yottabyte de información. Visto desde el aire, es indistinguible de un Centro de Detención de Inmigrantes: largos edificios sin ventanas rodeados de capas de seguridad de varias clases: cerrojos biométricos, controles marcados con alambre de espino y hombres armados con metralleta, muros y leyes federales de protección de secretos y de

propiedad intelectual. Los centros de datos de Inteligencia están legalmente borrados de los mapas por motivos de seguridad. El fotógrafo Trevor Paglen ha dedicado años de su vida a fotografiar ese tipo de lugares, usando objetivos de largo alcance y una lista de lugares secretos. Cuando salieron los documentos de Snowden, se dio cuenta de que «casi todos hablaban de infraestructura y que traían direcciones».[18]

Hace tiempo que la nube es más que el almacén de la World Wide Web. La pequeña semilla que plantó Tim Berners-Lee en su oficina del CERN ha sido devorada por un complejo sistema de procesamiento de datos donde se está produciendo la gran carrera armamentística del siglo XXI: el desarrollo de inteligencia artificial. Entre las principales funciones está almacenar gigantescas bases de datos y procesarlas con algoritmos de aprendizaje automático (*machine learning*) y profundo (*deep learning*) para terceros. «Amazon.com creó AWS para permitir a otras empresas disfrutar de la misma infraestructura —anuncia la web— con agilidad y beneficios de costes, y ahora sigue democratizando las tecnologías ML poniéndolas al alcance de todas las empresas». Cuanta más información de otros procesa, más aprende el algoritmo de Amazon y más poderoso es.

En el mundo de la inteligencia artificial, la cantidad de datos procesados es clave, pero hay material especialmente valioso. Los gobiernos ofrecen información especialmente detallada y útil, entre ella los golosos archivos clasificados de las agencias de inteligencia y sus extendidos sistemas de vigilancia. Microsoft Azure tiene un servicio de nube especial que vende «flexibilidad e innovación sin precedentes para las agencias gubernamentales de Estados Unidos y sus asociados», clasificado como Alto Secreto y con «capacidad cognitiva, inteligencia artificial y análisis predictivo». Un centenar de sus trabajadores se movilizaron para exigir a Bill Gates que renunciara a su contrato de 19,4 millones de dólares para procesar datos e imágenes para el Servicio de Inmigración y Control de Aduanas de Estados Unidos, después de ver que ayudaban a separar a las familias de inmigrantes de sus hijos. La empresa declaró que «Microsoft no está trabajando con el Departamento de Inmigración o la patrulla de fronteras en ningún proyecto *que implique separar a niños de sus familias en la frontera* y, contrariamente a los rumores, no tenemos conocimiento de que Azure o los servicios de Azure estén siendo utilizados con ese propósito». Pero no lo asegura, ni lo demuestra, ni se compromete a renunciar a su relación con el Pentágono, porque la sinergia entre las tecnológicas y las agencias federales funciona en las dos direcciones: aunque la empresa no pueda legalmente utilizar los datos

clasificados de manera directa, el procesado de esos datos proporciona nuevos niveles de precisión a sus algoritmos comerciales, que afinan sus habilidades predictivas para otros clientes.

Entre 2014 y 2016, Amazon ganó varios contratos con la CIA y la NSA para desarrollar un «entorno de fusión de big data» llamado Intelligence Community GovCloud. Uno de los hijos de su relación con la comunidad de inteligencia y las autoridades ha sido Rekognition, un software de reconocimiento facial automático capaz de identificar a más de un centenar de personas en una sola imagen. Los ejecutivos de Bezos ya le han dicho a sus empleados que no pierdan el tiempo protestando por darle servicio a Trump. «AWS está compitiendo a muerte por un contrato de diez mil millones con el Departamento de Defensa y no es casualidad que una de sus dos sedes esté a un kilómetro y medio del Pentágono —declaró Andy Jassy, responsable de AWS—. No vamos a desviarnos de ese negocio por las preocupaciones de ningún empleado». Se refiere al proyecto JEDI (Joint Enterprise Defense Incitiative), una infraestructura que centraliza todos los poderes del Departamento de Defensa en una sola isla-nube. Eso no significa que Amazon no tenga un código. En 2010, AWS sacó a Wikileaks de sus servidores por «incumplir los términos de uso al publicar contenido que no era suyo», pero no han tenido el mismo problema para trabajar con la firma más polémica de Silicon Valley: Palantir.

PALANTIR, EL BUSCAVIDAS

Peter Thiel era miembro de la PayPal Mafia, el «clan» de exalumnos de Standford y de la Universidad de Illinois que fundaron o trabajaron en Paypal y acabaron fundando algunas de las compañías más poderosas del Valle: Tesla, LinkedIn, Palantir Technologies, SpaceX, YouTube, Yelp.[19] Y había sido el primer inversor de Facebook, convirtiéndose en el mentor de Mark Zuckerberg y miembro destacado de su consejo de dirección. En 2004, Thiel puso treinta millones de dólares para fundar una empresa llamada Palantir Technologies Inc. El otro gran inversor fue la CIA, que puso dos millones a través de In-QTel, su fondo de capital riesgo para tecnologías que le serán útiles. Su objetivo era hacer minería de datos para el control de la población.

Un palantir es una piedra legendaria que permite observar a personas y momentos distantes en el tiempo y el espacio. Sauron la usa en *El señor de los anillos* para vigilar a sus enemigos, ver cosas que ya han ocurrido y enloquecer a sus víctimas con voces fantasmagóricas. La piedra está

conectada al anillo, que la «llama» cuando alguien lo usa. Siguiendo con la analogía, todo dispositivo conectado a internet está conectado a Palantir. Su primer trabajo para la NSA fue XKEYSCORE, un buscador capaz de atravesar correos, chats, historiales de navegación, fotos, documentos, webcams, análisis de tráfico, registros de teclado, claves de acceso al sistema con nombres de usuarios y contraseñas interceptados, túneles a sistemas, redes P2P, sesiones de Skype, mensajes de texto, contenido multimedia, geolocalización. Sirve para monitorizar a distancia a cualquier sujeto, organización o sistema, tirando de cualquier hilo: un nombre, un lugar, un número de teléfono, una matrícula de coche, una tarjeta. Siguiendo el patrón conocido, la tecnología que fue creada para vigilar «insurgentes» y «enemigos del mundo libre» en Irak y Afganistán fue rápidamente implementada en los estados federales para vigilar a los propios ciudadanos, especialmente en aquellos lugares donde hay mayoría afroamericana y en los más castigados por la pobreza o los huracanes, como Detroit o Nueva Orleans.

En la siguiente década, Palantir consiguió más de mil doscientos millones en contratos con la Marina, la Agencia de Inteligencia de Defensa, West Point, el FBI, la CIA, la NSA y los departamentos de Justicia, Hacienda, Inmigración y Seguridad Nacional. Incluso Medicaid tenía un proyecto piloto con ellos para investigar las llamadas de emergencia y otro para identificar servicios médicos ilegales en el sur. Esto durante la administración Obama. Después, Donald Trump ganó las elecciones con el apoyo público, técnico y financiero de dos personas: Peter Thiel y Robert Mercer, los respectivos dueños de Palantir y Cambridge Analytica. Hoy, Palantir es conocido como el Departamento de Precrimen de Trump, porque su tecnología predictiva es utilizada por la policía para detectar «zonas de calor» donde podría estallar la violencia. También detecta grupos o personas «de interés», que hayan asistido a manifestaciones, participado en huelgas, tengan amigos en Greenpeace, usen tecnologías de encriptación o hayan apoyado a otros activistas en redes sociales. Palantir tiene acceso a huellas y otros datos biométricos, archivos médicos, historial de compras con tarjetas, registros de viajes, conversaciones telefónicas, impuestos, historiales de menores. Y se queda con todos los datos que procesa, para usarlos con otros clientes como las agencias de inteligencia de Inglaterra, Australia, Nueva Zelanda y Canadá. En Europa, es utilizado por al menos dos gobiernos, el británico y el danés. Pero sobre todo se ha convertido en el juguete de Trump para la detención y deportación masiva de inmigrantes sin antecedentes criminales. Todo está alojado en Amazon Web

Services, que también usa Amazon Rekognition, su algoritmo de reconocimiento facial.

La banalización de la vigilancia

En mayo de 2018, Taylor Swift puso una carpa de fotos y vídeos en el estadio Rose Bowl de Los Ángeles donde daba un concierto, para amenizar a sus fans. Meses más tarde, la revista *Rolling Stone* publicó que el espacio estaba secretamente equipado con software de reconocimiento facial que tomaba fotos de los asistentes y las enviaba a un servidor en Nashville, para compararlas con una base de datos de personas sospechosas de acosar a la cantante. Esas personas podrían ser «el número de hombres que tenemos registrados por haber aparecido por mi casa, la casa de mi madre, o los que han amenazado con matarme, secuestrarme o casarse conmigo» que mencionó la cantante en una entrevista,[20] o cualquier otra lista de cualquier otra base de datos de cualquier otra empresa o institución. No podemos saberlo. Pero introduce una nueva carga poética en el nombre de la gira de su disco: «Mira lo que me has hecho hacer».

Los algoritmos de reconocimiento facial son el trozo de código más valioso del mundo y el más peligroso. Ofrecen un sistema de reconocimiento involuntario e invisible, diseñado para identificar personas sin que se den cuenta, sin su permiso y sin que puedan ofrecer resistencia, porque son traicionados por las características irrenunciables e inalterables de su físico. Aunque la regulación de ese tipo de datos varía enormemente de un país a otro, su uso ha explotado en todas las industrias porque el acceso es sencillo e inmediato. «Amazon Rekognition facilita la incorporación del análisis de imágenes y vídeos a sus aplicaciones. Usted tan solo debe suministrar una imagen o vídeo a la API de Rekognition y el servicio identificará objetos, personas, texto, escenas y actividades». ¡Los primeros mil minutos de vídeo al mes son gratuitos! La misma tecnología que usa el ejército para encontrar terroristas y vigilar zonas de conflicto desde un dron, o las autoridades portuarias en los arcos de los aeropuertos, está disponible para tiendas, centros comerciales, bancos, garajes, festivales de música, gasolineras, colegios privados y parques temáticos. C-SPAN, el canal que retransmite en directo todo lo que pasa en el Congreso estadounidense, usa Amazon Rekognition para identificar automáticamente a los parlamentarios; Sky News lo usó para identificar a los invitados de la boda del Príncipe Harry y Meghan Markle, sobrevolando la capilla de St. George con una flota de drones.

Madison Square Garden, el estadio de Manhattan con capacidad para veintidós mil personas donde juegan los Knicks, toca Billy Joel y se entregan los Grammy cada año, lo usa como parte de su protocolo normal de seguridad. Cada nuevo usuario pone un nuevo ojo en la red de vigilancia de Amazon, que extiende sus dominios y agudiza sus habilidades para ponerlas al servicio de sus valiosos clientes, como Palantir.

Hasta hace poco, el mejor algoritmo de reconocimiento facial era el de Facebook. DeepFace tiene un porcentaje de acierto del 97,47 por ciento, gracias al esfuerzo de los usuarios. En enero de 2011, antes de que el sistema empezara a sugerir los nombres, un usuario normal quedaba etiquetado en una media de 53 fotos, una decena más de las que son necesarias para que el algoritmo genere un modelo. El 2016 «liberó» sus algoritmos de detección, reconocimiento y clasificación de fotografía DeepMask, SharpMask y MultiPathNet para que todo el mundo pudiera utilizarlos en plataformas como Flickr, añadiendo astutamente nuevas bases de datos a su amplia colección. Por poner en contexto sus capacidades, el algoritmo diseñado por el FBI acierta solo el 85 por ciento y el ojo humano no pasa del 97,65 por ciento. Una de sus funciones es reconocer y etiquetar a las personas que salen en una imagen, incluso cuando la persona que ha subido la foto no sepa quién es. Otra es reconocer a cualquier persona haciendo cualquier cosa cuando no está conectada, en la vida real.

En 2015, un fotógrafo ruso llamado Egor Tsevtkov empezó a hacer fotos de personas que veía en el metro y a conectarlas con sus perfiles en VKontakte, el Facebook ruso, usando una aplicación gratuita llamada FindFace. Verdaderamente, no era más que una copia del Face Finder de Facebook que permite encontrar a tus amigos a través de fotos, pero que estaba restringido a aquellos que ya estaban en tu círculo de amigos. Su proyecto «Tu cara es big data» demostró que estar en las redes sociales en la era del reconocimiento facial significa que cualquiera que te hace una foto por la calle puede saber inmediatamente quién eres y contactarte. Si quieres llevarlo más lejos, también puede comprar la información a un *data broker* y saberlo todo sobre ti. Google lanzó su FaceNet en 2015. Tanto Android como iPhone ofrecen sistemas de reconocimiento facial para desbloquear el teléfono pero, técnicamente, cualquier aplicación que use la cámara puede agregar datos a un software de reconocimiento facial. El proyecto llamó la atención del Kremlin, que financió generosamente a su joven programador Alexander Kabakov y su empresa Ntechlab para seguir desarrollando. Hoy es una de las principales firmas internacionales del sector.

De hecho, las aplicaciones de realidad aumentada son la manera más fácil de mapear las caras de los usuarios, el Foursquare de la identificación invisible. Los populares filtros de Snapchat y de Instagram para ponerse orejas de conejito, fondos de animación o cutis de porcelana lo hacen. En 2017 Apple lanzó una aplicación similar llamada Clipps. En Asia, la reina es Face++, el filtro embellecedor que todo el mundo usa antes de enviar, compartir o publicar una foto. Cada vez que usamos estas aplicaciones o subimos fotos a la nube, estamos entrenando los mismos algoritmos que usan las empresas para abrir la puerta a sus empleados, los sistemas de transporte para cobrar un viaje o el que usan los cajeros como identificación para sacar dinero o pagar en un restaurante. Y que nos identifican aunque no queramos, tanto si lo sabemos como si lo ignoramos. «No solo pueden pagar las cosas de esta manera, sino que el personal del café es alertado de su presencia por el sistema para poder saludarlo con su nombre», explicaba el profesor de los programadores de Face++ en la revista del MIT.[21] También es parte de la tupida red de vigilancia del Gobierno chino, donde no puedes dar un paso sin que te ponga o quite puntos de crédito social.

China 2020, La primera dictadura digital

En Beijing, un ciudadano que cruza en rojo puede ser multado instantáneamente en su cuenta bancaria. También puede verse inmortalizado en un *loop* de vídeo cruzando indebidamente en las marquesinas de las paradas de autobús, para escarnio propio y de su familia. Si comete más infracciones, como aparcar mal, criticar al Gobierno en una conversación privada con su madre o comprar más alcohol que pañales, podría perder el empleo, el seguro médico y encontrarse con que ya no puede conseguir otro trabajo ni coger un avión. Así es como funcionará el nuevo sistema de crédito social chino, programado para entrar completamente en vigor en 2020. Su lema es: «Los buenos ciudadanos caminarán libres bajo el sol y los malos no podrán dar un paso».

En el sistema de crédito social, también conocido como Sesame Credit, todos los ciudadanos empiezan con la misma puntuación, pero después va subiendo o bajando en función de cómo se portan. Entre las muchas cosas que bajan puntuación están robar, comer en el metro, empezar una pelea, orinar en la calle y dejar de pagar las facturas. También hablar mal del Gobierno en un chat privado con un amigo, reunirse con intenciones sindicales, participar en manifestaciones políticas, entrar en una mezquita (aunque sea en otro país) o

leer libros inapropiados. Hacer trampas en los videojuegos (usando bots) quita muchos puntos. También relacionarse con personas con puntuación muy baja, aunque sean miembros de la familia más cercana. A medida que va perdiendo crédito, el mal ciudadano pierde acceso a servicios, trabajos, casas, promociones, hipotecas, el derecho a coger el tren o acudir a un concierto. En junio de 2018, un total de 169 personas fueron expulsadas del sistema ferroviario y también perdieron permiso para volar. Sus delitos, que fueron publicados por el Gobierno junto con sus nombres y sus caras, incluyeron deudas, provocaciones y, al menos en un caso, tratar de cruzar el arco de control del aeropuerto con un mechero encima. También hay cosas que suben puntos: sacar buenas notas, donar sangre, trabajar como voluntario o participar en las actividades que organiza el Gobierno local y hacer horas extras en el trabajo. Los ciudadanos con muchos puntos pueden saltarse las colas del hospital, reciben descuentos especiales, promociones laborales y hasta acceso a páginas de contactos para conseguir citas con chicas «muy bien». Reciben créditos para comprar casas en los mejores barrios y matrículas para sus hijos en los mejores colegios. Zhenai.com, el Tinder chino, ofrece visibilidad a los hombres con puntuación más alta. Todo el mundo conoce el crédito actualizado de todos los demás. Uno tiene que saber con quién se relaciona.

El sistema de crédito chino depende de más de cuatrocientos millones de cámaras que vigilan permanentemente a la población, todas conectadas a servidores con sistemas de reconocimiento facial en tiempo real. Forma parte de un programa llamado Sharp Eye, pero en realidad cualquier cámara, micrófono o sensor de cualquier dispositivo chino en cualquier lugar es parte del sistema de vigilancia del Gobierno, incluidos los teléfonos móviles. La nueva Ley de Ciberseguridad, aprobada en 2017, reclama soberanía nacional sobre el ciberespacio y obliga a las tecnológicas a vigilar a los usuarios, compartir con las autoridades los códigos fuente de todos sus programas y abrir sus servidores para revisiones de seguridad. Además de sacar dinero presentando el rostro en lugar de la tarjeta, la mayor parte de la población cobra, presta y gasta a través de aplicaciones móviles como WeChat Pay y Alipay. La digitalización total de las transacciones es fundamental para el registro y control del Gobierno. Como dice la protagonista en *El cuento de la criada*, el salto de la democracia a la dictadura es fácil cuando todo el dinero es digital. Todo el proyecto se sostiene gracias a un ecosistema de empresas tecnológicas dominado por tres gigantes: Baidu, Tencent y Alibaba. Hubo un tiempo en que no eran más que copias sin personalidad de las páginas

populares estadounidenses. Todo eso acabó el día que el presidente de la República Popular China Xi Jinping vio cómo una inteligencia artificial extranjera les ganaba al Go.