

Mario Saavedra

La batalla de configurar el mundo digital con unas reglas u otras.



Así pasó con la lucha contra la discriminación racial, o la de las mujeres, o más recientemente con la del matrimonio gay. Siempre hay primero unos pocos que dan un paso adelante, y son considerados unos excéntricos. En 1955, Rosa Park se negó a ceder su asiento de la zona para negros a un blanco, una vez que la clase preferente se había llenado. Fue detenida.

Seis décadas después, Edward Snowden, el informante que ha destapado un escándalo de vigilancia masiva que deja en un simple juego de niños el *Watergate* de Richard Nixon, ha tenido que exiliarse en Rusia, acusado de espionaje y de robo de la propiedad del Estado. El periodista que reveló el caso, Glenn Greenwald, ha sido presionado por el Gobierno estadounidense, que ha ordenado interrogar a su pareja durante nueve horas en base al

Terrorist Act; y los medios conservadores le consideran un traidor.

Mientras, la organización de derechos civiles más importante de Estados Unidos, la ACLU, se prepara para intensificar sus acciones porque “ha llegado el momento de frenar el Estado vigilante (*surveillance state*)”.

Julian Assange permanece refugiado en la embajada de Ecuador para evitar ser extraditado por un presunto delito sexual que él considera una excusa para hacerle pagar por haber facilitado la mayor filtración de documentos digitales clasificados de la Historia. Bradley Manning, ahora Chelsea, ha sido condenado a 35 años de cárcel por robo de documentos del Estado. Entre ellos, los de la guerra de Afganistán (*warlogs*) que mostraban cómo el Gobierno estadounidense mintió con las cifras de bajas civiles; centenares de miles de cables diplomáticos (el *CableGate*), y vídeos en los que el Ejército de EE UU asesinaba desde el aire a grupos de personas desarmadas, entre ellas dos reporteros de la agencia de noticias Reuters.

Más allá de la consideración moral que puedan merecer cada uno de los personajes antes citados (y todos tienen claroscuros, el más obvio el de Assange, que eventualmente puso en peligro a miles de informantes de Estados Unidos al no censurar lo publicado), lo cierto es que todos son protagonistas de una nueva guerra, una lucha entre ciudadanos particulares y unos gobiernos, el estadounidense en particular, que tratan de silenciarlos, entre otras cosas porque han roto la ley.

Se trata, sobre todo, de un cambio generacional importante. La gente que ahora está en sus cuarenta, y que detendrá el poder o ahora o en las próximas dos décadas, nació y creció en un mundo esencialmente analógico. Vio surgir de la nada el mundo digital. Lo ha visto crecer, y ahora tienen que regularlo, legislarlo y aprovecharlo económicamente.

Hasta principios de los 80 no se empezaron a reemplazar de forma sistemática las máquinas de escribir por los ordenadores personales. De eso hace tan sólo 30 años. Un suspiro en términos históricos. Solo a principios de los 90 llegaron las computadoras a los hogares, y aún entonces el nivel de información guardado era escaso. En realidad, llevamos volcando nuestra información privada en el mundo digital, realizando transacciones, compras y comunicándonos sólo un par de décadas, en el mejor de los casos.

Todo está en pañales, y por ello hay mucho margen para marcar la impronta, levantar el mundo digital con unas reglas u otras. Un ejemplo: el correo es inviolable en casi todos los países, y abrirlo es ilegal, incluso para las agencias de espionaje, que precisan de una orden judicial. El correo electrónico, sin embargo, es espiado sistemáticamente por los servicios de inteligencia, o escaneado sin pudor por las compañías como Google o por otras encargadas de gestionar la publicidad. La desincronización entre uno y otro mundo es obvia. Es en esa tierra de nadie en la

que se combate por configurar el mundo digital en uno u otro sentido.

Internet, por ejemplo. No tiene aun esencialmente demasiada regulación, ni falta que parece hacerle: es el avance tecnológico más rápidamente absorbido por la población de la Historia. Las Naciones Unidas llevan desde 2006 tratando de crear una legislación marco internacional. En la última reunión, en Bali 2013, del Foro de Gobernanza de Internet de la ONU quedó claro que países poco amigos de la privacidad y los derechos civiles como Rusia están muy interesados en ponerle puertas a ese campo virtual. Internet es el principal enemigo de los regímenes autoritarios o dictatoriales (China, Irán, Egipto, Rusia, entre otros muchos). Pero no son sólo ellos los que pelean por controlarlo.

Todos los presidentes de Estados Unidos han increpado, en uno u otro momento, a China por sus ciberataques o por la intervención impúdica del Gobierno chino en los ordenadores de sus ciudadanos y de los del resto del mundo. Llegaron incluso a hacer público un informe, a través de una de sus empresas contratistas, en las que acusaban directamente a Pekín de estar detrás de los ataques. Unos meses después de la campaña, Edward Snowden, expuso la tremenda hipocresía de Washington, el espía *in chief*, que no conoce límites a la intromisión en la información de los ciudadanos y corporaciones del mundo a través de su Agencia de Seguridad Nacional (NSA, en sus siglas en inglés).

El ritmo de descubrimientos sobre la profundidad y extensión de la cibervigilancia es de vértigo. Hay asuntos prosaicos como el LoveInt, la *inteligencia del amor*, funcionarios de la NSA que utilizaban el poderoso sistema de la agencia para espiar a sus seres queridos. Hay otros demás impacto político, como los pinchazos de los teléfonos personales de prácticamente todolíder político relevante para Estados Unidos. Por el camino, se ha descubierto que los espías anglosajones (en una coalición llamada los Cinco Ojos, formada por Estados Unidos, Reino Unido, Canadá, Nueva Zelanda y Australia) empleaban todo método posible para obtener toda la información digital abarcable, desde videojuegos como Angry Birds hasta dispositivos implantados en al menos 100.000 ordenadores fabricados en el país y que permiten espiar el contenido incluso cuando no está conectado a la Red. Reino Unido, por su parte, pinchaba directamente los cables que pasan por sus islas hacia Europa y copiaba toda la información en unos mega servidores, para después usarla a su antojo. Ponían, además, los más clásicos micrófonos en las cumbres políticas, en la sede de la Unión Europea en Bruselas, en la embajada en Washington. Estados Unidos tenía puertas traseras en los servidores de las grandes empresas de Internet o de computación como Google, Microsoft, Facebook o Apple, entre otras muchas, y acuerdos concretos con las compañías de telecomunicaciones como ATyT. Mientras, la NSA prepara en el desierto de Utah un enorme centro de datos destinado a convertirse en el cerebro de la bestia de control digital.

Y son sólo los primeros pasos. La tecnología aún es burda. Por ejemplo, se cree que la NSA aún no puede romper todos los códigos de encriptación. Por eso tuvieron que utilizar a los jueces para obligar a empresas como Lavabit, que se dedicaba dar servicios de encriptado de e-mail y a la que obligaron a entregar las reglas de encriptado (SSL) al Gobierno. Y por eso intentan sin mucho éxito conseguir un ordenador cuántico que rompería cualquier código.

Pero la lucha no está en marcha sólo en el terreno de la privacidad. En estos momentos hay un enfrentamiento abierto entre la administración Obama y las empresas como Netflix o Google, por un lado, y las de telecomunicaciones por otro, sobre la llamada “neutralidad web”. Washington y las compañías de contenidos creen que las operadoras deben tratar igual a todo el contenido. Un juez ha decidido que no, que Verizon por ejemplo puede cobrar más a Netflix, que ocupa más ancho de banda. Los activistas, como Free Press, han puesto el grito en el cielo: es el primer paso para la creación de *gatekeepers*, operadoras que decidan castigar o premiar a un contenido o a otro.

El debate es feroz. Por un lado está el manido argumento del equilibrio entre la privacidad y la seguridad. Esta oleada de compulsión de control lleva siglos implantada en los gobiernos. J. Edgar Hoover, el obsesivo jefe del FBI, tenía controlado no sólo a disidentes, sino a políticos y artistas. Pero el mundo digital amplía de manera insospechada las posibilidades de crear

ficheros similares a los de Hoover sobre todos y cada uno de los ciudadanos del mundo.

La obsesión por el espionaje cibernético explotó en Estados Unidos tras los atentados del 11 de septiembre, y se escuda en ellos desde entonces. La Patriot Act cambió por completo el panorama, hasta entonces dominado por las enmiendas que protegen a los ciudadanos de abusos gubernamentales como los registros indiscriminados. La línea directriz de esta ley era que la balanza entre lo que el gobierno debe saber para proteger a los ciudadanos, y su derecho de no ser espiados, había oscilado demasiado del lado de estos últimos.

En realidad, la propia eficacia del espionaje masivo está en entredicho. Tras las revelaciones de Snowden, la Casa Blanca ha asegurado por activa y por pasiva que ha servido para luchar contra el terrorismo. Hablan en concreto del programa bajo la sección 702 del *Foreign Intelligence Surveillance Act*. En octubre de 2013, se hizo pública la primera información sobre el uso del contenido de los correos electrónicos contra un presunto terrorista, Jamshid Muhtorov. “Sabemos de al menos 50 amenazas que se han evitado gracias al uso de esta información, no sólo en Estados Unidos, sino también en Alemania. Se han salvado vidas”, aseguró Obama en una visita al país teutón.

Sin embargo, muchos consideran simple propaganda esas frases. Un análisis detallado de los 225 casos de terrorismo contra miembros de Al Qaeda abiertos en Estados Unidos desde 2001, realizado por la *New America Foundation*, revela que “los métodos de investigación tradicionales, como el uso de informantes, avisos de las comunidades locales, y misiones concretas de inteligencia han sido los que han generado el ímpetu de la investigación en la mayoría de los casos, mientras que la contribución del programa de espionaje masivo de la NSA ha sido mínima”. En la misma línea se han manifestado varios senadores con acceso a la información clasificada del Gobierno. La idea básica es que pagar a un informante suele ser infinitamente más productivo que guardar los datos de todas las llamadas hechas por centenares de millones de personas en todo el mundo o el contenido de sus correos electrónicos. Osama Bin Laden no usaba e-mail. Fue capturado gracias a la información pagada sobre la identidad de uno de sus *hombres-correo*.

El impacto de las revelaciones de espionaje masivo (a ciudadanos, empresas y líderes políticos) ha sentado especialmente mal en países como Alemania, con un reciente pasado de *Estados vigilantes*. Los archivos del ministerio de Seguridad del Estado (*Stasi*) aún contienen ficheros de gran parte de los adultos alemanes. Pero lo mismo ha ocurrido en Estados Unidos. El 66% se muestran preocupados por la recolección de los datos de sus llamadas, según una encuesta del diario *The Washington Post*. El 60% asegura que valora su privacidad por encima de la amenaza terrorista. El 61% considera que Snowden hizo un buen servicio a Estados

Unidos, según una encuesta de *The Economist*.

La reacción del gobierno de Barack Obama ha sido esencialmente de relaciones públicas. Ha comparecido durante más de una hora para hablar sobre el escándalo de la NSA. Sin embargo, ha rechazado la mayoría de las recomendaciones del informe de expertos que él mismo encargó. Se debate sobre quién tiene que guardar los datos, si el Gobierno o el sector privado, pero no quiere detener el programa de recolección indiscriminada de datos.

La próxima década va a estar plagada de protagonistas como Snowden, Manning, Assange y va a suponer un reto para asociaciones que hasta ahora tenían un trabajo de segunda magnitud, como la ACLU o las organizaciones de defensa de Internet. Del resultado de esta batalla de derechos civiles dependerá el mundo digital que nos viene.

Artículos relacionados

- [La datificación de la realidad.](#) **Lino González**
- [‘Hackear’ la diplomacia.](#) **Juan Luis Manfredi**
- [Dejar de espiar a sus aliados.](#) **Mario Saavedra**
- [Las multinacionales gobernarán el mundo.](#) **Hal Varian**
- [Ciberespeluznante: amenazas en la red.](#) **Eugene Kaspersky**
- [Del mundo virtual al mundo real.](#) **Yoani Sánchez**
- [Depende: ciberguerra.](#) **Thomas Rid**

Fecha de creación

21 febrero, 2014