EDWARD SNOWDEN, LA NSA Y EL ESTADO DE VIGILANCIA DE EE.UU.

SNOWDEN

SIN UN LUGAR DONDE ESCONDERSE

GLENN GREENWALD

El periodista de investigacion de The Guardian y autor superventas Glenn Greenwald, ofrece una mirada en profundidad sobre el escandalo de la NSA que ha provocado un gran debate sobre la seguridad nacional y la privacidad de la información. Con nuevas revelaciones de los documentos confiados a Glenn Greenwald por el propio Edward Snowden, este libro explora la extraordinaria cooperacion entre la industria privada y la NSA, y las consecuencias de largo alcance del programa de vigilancia del gobierno, tanto a nivel nacional como en el extranjero.

Este libro está dedicado a todos aquellos que han querido
arrojar luz sobre los sistemas de vigilancia secreta del gobierno de Estados Unidos, en especial a los valientes
filtradores que para ello han arriesgado su libertad.

El gobierno de Estados Unidos ha perfeccionado una capacidad tecnológica que nos permite controlar los mensajes que van por el aire… Esta capacidad puede en cualquier momento volverse en contra del pueblo norteamericano, y a ningún norteamericano le quedaría privacidad alguna, tal es la capacidad de controlarlo todo… conversaciones telefónicas, telegramas, lo que sea. No habría un lugar donde esconderse.

Senador Frank Church, presidente del Comité del Senado
para Estudiar Operaciones Gubernamentales con Respecto
a Actividades de Inteligencia, 1975

Introducción

En el otoño de 2005, sin grandes expectativas a la vista, decidí crear un blog político. En su momento apenas calibré el grado en que esta decisión me cambiaría la vida a la larga. Mi principal motivación era la creciente inquietud que me causaban las teorías extremistas y radicales sobre el poder adoptadas por el gobierno de EE.UU. tras el 11 de Septiembre, y esperaba que escribir sobre estos asuntos me permitiera causar un impacto mayor que el de mi labor de entonces como abogado de derechos civiles y constitucionales.

Solo siete semanas después de empezar a bloguear, el *New York Times* dejó caer un bombazo: en 2001, decía, la administración Bush había ordenado a la Agencia de Seguridad Nacional (NSA) escuchar en secreto las comunicaciones electrónicas de los norteamericanos sin las órdenes judiciales requeridas por la ley penal pertinente. En el momento en que salieron a la luz estas escuchas sin orden judicial llevaban realizándose ya desde hacía cuatro años y mediante ellas se había espiado a varios miles de norteamericanos.

El tema constituía una convergencia perfecta entre mis pasiones y mis conocimientos. El gobierno intentaba justificar el programa secreto de la NSA recurriendo exactamente al tipo de teoría extrema del poder ejecutivo que me había impulsado a empezar a escribir: la idea de que la amenaza del terrorismo otorgaba al presidente una autoridad prácticamente ilimitada para hacer lo que fuera preciso a fin de «mantener segura la nación», incluida la autoridad

para infringir la ley. El debate subsiguiente conllevó complejas cuestiones de derecho constitucional e interpretaciones legales, que mi formación me permitía abordar con cierto conocimiento de causa.

Pasé los dos años siguientes cubriendo todos los aspectos del escándalo de las escuchas ilegales de la NSA, tanto en mi blog como en mi libro superventas de 2006. Mi postura era muy clara: al ordenar escuchas sin autorización judicial, el presidente había cometido delitos y debía asumir su responsabilidad. En el ambiente político cada vez más opresivo y patriotero de Norteamérica, mi actitud resultó de lo más controvertida.

Fueron estos antecedentes los que, unos años después, movieron a Edward Snowden a escogerme como primer contacto para revelar las fechorías de la NSA a una escala aún mayor. Dijo creer que yo entendería los peligros de la vigilancia masiva y los secretos de estado extremos, y que no me volvería atrás ante las presiones del gobierno y sus numerosos aliados en los medios y otros sectores.

El extraordinario volumen de los documentos secretos que me pasó Snowden, junto con el dramatismo que le ha rodeado a él, han generado un interés mundial sin precedentes en la amenaza de la vigilancia electrónica y el valor de la privacidad en la era digital. Sin embargo, los problemas subyacentes llevan años recrudeciéndose, casi siempre en la oscuridad.

En la actual polémica sobre la NSA hay sin duda muchos aspectos exclusivos. La tecnología permite actualmente un tipo de vigilancia omnipresente que antes era terreno acotado solo de los escritores de ciencia ficción más imaginativos. Además, tras el 11-S, el culto norteamericano a la seguridad ha creado más que nada un ambiente especialmente propicio a los abusos de poder. Y gracias a la valentía de Snowden y a la relativa facilidad para copiar información digital, tenemos un incomparable vistazo de primera

mano sobre los detalles de cómo funciona realmente el sistema de vigilancia.

Aun así, las cuestiones planteadas por la historia de la NSA se hacen, en muchos aspectos, eco de numerosos episodios del pasado, pasado que se remonta a varios siglos. De hecho, la oposición a que el gobierno invadiera la privacidad de la gente fue un factor importante en la creación de Estados Unidos, pues los colonos protestaban contra las leyes que permitían a los funcionarios británicos registrar a voluntad cualquier domicilio. Era legítimo, admitían los colonos, que el estado obtuviera órdenes judiciales específicas, seleccionadas, para detener a individuos cuando hubiera indicios de causas probables de actos delictivos. No obstante, las órdenes judiciales de carácter general —el hecho de que todos los ciudadanos fueran objeto potencial de registro domiciliario indiscriminado— eran intrínsecamente ilegítimas.

La Cuarta Enmienda consagró esta idea en las leyes norteamericanas. El lenguaje es claro y conciso: «El derecho de la gente a tener seguridad en sus personas, casas, papeles y efectos, contra cualquier registro y arresto irrazonable, no será violado, y no se emitirá ningún mandamiento, a no ser que exista causa probable, apoyada por un juramento o testimonio, y que describa especialmente el lugar a ser registrado, las personas a ser arrestadas y las cosas a ser confiscadas». Se pretendía, por encima de todo, suprimir para siempre en Norteamérica el poder del gobierno para someter a sus ciudadanos a vigilancia generalizada si no mediaban sospechas.

En el siglo XVIII, el conflicto con la vigilancia se centraba en los registros domiciliarios, pero, a medida que la tecnología fue evolucionando, la vigilancia evolucionó también. A mediados del siglo XX, cuando la extensión del ferrocarril empezó a permitir el reparto rápido y barato del correo, la furtiva violación del mismo por el gobierno británico provocó un grave escándalo en Reino Unido. En las primeras dé-

cadas del siglo XX, la Oficina de Investigación de EE.UU. —precursora del actual FBI— utilizaba escuchas telefónicas, además de informantes y control de la correspondencia, para perseguir a quienes se opusieran a la política gubernamental.

Con independencia de las técnicas específicas utilizadas, desde el punto de vista histórico la vigilancia masiva ha tenido varias características constantes. Al principio, los más afectados por la vigilancia siempre son los disidentes y los marginados, por lo que quienes respaldan al gobierno o se muestran indiferentes sin más acaso lleguen a creer equivocadamente que son inmunes. Pero la historia demuestra que la mera existencia de un aparato de vigilancia a gran escala, al margen de cómo se utilice, es en sí mismo suficiente para reprimir a los discrepantes. Una ciudadanía consciente de estar siempre vigilada enseguida se vuelve dócil y miedosa.

Una investigación de Frank Church de mediados de la década de 1970 sobre espionaje del FBI puso de manifiesto que la agencia había etiquetado a medio millón de ciudadanos norteamericanos como «subversivos» potenciales y había espiado de manera rutinaria a montones de personas basándose únicamente en el criterio de las ideas políticas. (La lista de objetivos del FBI iba de Martin Luther King a John Lennon, pasando por el Movimiento de Liberación de las Mujeres o la Sociedad John Birch). De todos modos, la plaga de abusos de vigilancia no es ni mucho menos exclusiva de la historia norteamericana. La vigilancia masiva ha sido una tentación universal para cualquier poder sin escrúpulos. Y el motivo es el mismo en todos los casos: neutralizar a la disidencia y exigir conformidad.

Así pues, la vigilancia une a gobiernos de, por lo demás, credos políticos notablemente distintos. A comienzos del siglo XX, los imperios francés y británico crearon departamentos especializados de control para hacer frente a la amenaza de los movimientos anticolonialistas. Tras la Se-

gunda Guerra Mundial, el Ministerio para la Seguridad del Estado de Alemania Oriental, conocido popularmente como Stasi, llegó a ser sinónimo de intrusión gubernamental en la vida privada. Y más recientemente, cuando las protestas populares de la Primavera Árabe pusieron en jaque el poder de los dictadores, los regímenes de Siria, Egipto y Libia empezaron a espiar el uso que los opositores internos hacían de internet.

Las investigaciones de Bloomberg News y el *Wall Street Journal* han demostrado que, cuando estas dictaduras estaban siendo arrolladas por las protestas, fueron literalmente a comprar instrumentos de vigilancia a las empresas tecnológicas occidentales. El régimen sirio de Assad mandó llamar a empleados de la empresa italiana de vigilancia Area SpA, a quienes se dijo que los sirios «necesitaban rastrear personas urgentemente». En Egipto, la policía secreta de Mubarak compró herramientas para penetrar en la encriptación de Skype e interceptar llamadas de activistas. Y en Libia, decía el *Journal*, varios periodistas y rebeldes que en 2011 entraron en un centro de control del gobierno descubrieron «un muro de aparatos negros del tamaño de neveras» de la empresa francesa de vigilancia Amesys. El equipo «inspeccionaba el tráfico en internet» del principal proveedor de servicios de internet en Libia, «abriendo e-mails, descifrando contraseñas, husmeando en chats online y cartografiando conexiones entre varios sospechosos».

La capacidad para escuchar a escondidas las comunicaciones de la gente confiere un poder inmenso a quienes lo hacen. Y a menos que ese poder esté sometido a una supervisión y una rendición de cuentas rigurosas, casi seguro que servirá para cometer abusos. Esperar que el gobierno de EE.UU. haga funcionar una máquina de vigilancia masiva en completo secreto sin caer en sus tentaciones contradice todos los ejemplos históricos y los datos disponibles sobre la naturaleza humana.

De hecho, antes incluso de las revelaciones de Snowden ya estaba claro que considerar a Estados Unidos una excepción en el asunto de la vigilancia era una postura muy ingenua. En 2006, en una sesión del Congreso titulada «Internet en China: ¿herramienta para la libertad o prohibición?», los oradores criticaron al unísono a las empresas tecnológicas norteamericanas que ayudaban al gobierno chino a eliminar la disidencia en internet. Christopher Smith (R-NJ), el congresista que presidía la sesión, comparó la cooperación de Yahoo! con la policía secreta china con la entrega de Ana Frank a los nazis. Fue una arenga a pleno pulmón, una actuación típica de los funcionarios norteamericanos cuando hablan de un régimen no alineado con EE.UU.

Sin embargo, a los asistentes a la sesión tampoco se les pasaría por alto que la sesión se celebraba precisamente dos meses después de que el *New York Times* revelase las numerosísimas escuchas telefónicas internas sin orden judicial llevadas a cabo por la administración Bush. En vista de esas revelaciones, denunciar a otros países por realizar su propia vigilancia interna sonaba bastante falso. El representante Brad Sherman (D-CA), que tomó la palabra después de Smith, señaló que las empresas tecnológicas a las que se les dice que opongan resistencia al régimen chino también deberían ser prudentes con su propio gobierno. «De lo contrario», profetizaba, «mientras los chinos verán su privacidad violada de la manera más abyecta, aquí en Estados Unidos quizás un día tengamos un presidente que, amparándose en estas laxas interpretaciones de la Constitución, lea nuestro correo electrónico; y yo preferiría que para eso hiciera falta una orden judicial».

A lo largo de las décadas pasadas, el miedo al terrorismo —avivado por sistemáticas exageraciones de la amenaza real— ha sido aprovechado por dirigentes norteamericanos para justificar una amplia serie de políticas extremas: ha dado lugar a guerras de agresión, a un régimen que tortura en todo el mundo y a la detención (incluso el asesinato) de

ciudadanos tanto extranjeros como norteamericanos sin mediar acusación alguna. Pero el ubicuo y secreto sistema de vigilancia a no sospechosos que se ha generado puede muy bien resultar su legado más duradero. Y ello porque, pese a todos los paralelismos históricos, existe también una dimensión realmente nueva en el actual escándalo de la vigilancia de la NSA: el papel desempeñado actualmente por internet en la vida cotidiana.

Sobre todo para la generación más joven, internet no es un ámbito separado, autónomo, donde se llevan a cabo unas cuantas funciones vitales. No consiste solo en el teléfono y la oficina de correos. Es el epicentro del mundo, el lugar en el que ocurre prácticamente todo. Donde se hacen amigos, donde se escogen libros y películas, donde se organiza el activismo político, donde se crean y almacenan los datos más privados. Es donde se desarrolla y expresa la verdadera personalidad y la identidad de la persona.

Transformar *esta* red en un sistema de vigilancia de masas tiene repercusiones distintas de las de otros programas anteriores de vigilancia estatal. Los sistemas de espionaje precedentes eran necesariamente más limitados, y era más fácil eludirlos. Permitir a la vigilancia arraigar en internet significaría someter prácticamente todas las formas de interacción humana, la planificación e incluso el pensamiento propiamente dicho a un control estatal exhaustivo.

Desde la época en que internet empezó a utilizarse ampliamente, muchos han detectado su extraordinario potencial: la capacidad para liberar a centenares de millones de personas democratizando el discurso político e igualando el campo de juego entre los poderosos y los carentes de poder. La libertad en internet —la capacidad de usar la red sin restricciones institucionales, control social o estatal, ni miedo generalizado— es fundamental para el cumplimiento de esa promesa. Por tanto, convertir internet en un sistema de vigilancia destruye su potencial básico. Peor aún, transforma la red en un instrumento de represión, lo cual

amenaza con crear al arma más extrema y opresora de la intrusión estatal que haya visto la historia humana.

Por esto las revelaciones de Snowden son asombrosas y de vital importancia. Al atreverse a exponer las pasmosas capacidades de vigilancia de la NSA y sus ambiciones aún más increíbles, Snowden ha dejado claro que nos hallamos en una encrucijada histórica. ¿Será la era digital el preludio de la liberación individual y de las libertades políticas que solo internet es capaz de promover? ¿O bien esto dará origen a un sistema de control y seguimiento omnipresentes, que superará los sueños de los peores tiranos del pasado? Ahora mismo, cualquier camino es posible. Nuestras acciones determinarán dónde terminaremos.

1

CONTACTO

El 1 de diciembre de 2012 recibí la primera comunicación de Edward Snowden, aunque en ese momento no tenía ni idea de que era suya.

El contacto llegó en forma de e-mail de alguien que se llamaba a sí mismo Cincinnatus, una alusión a Lucius Quinctius Cincinnatus, el agricultor romano que, en el siglo V a.C., fue nombrado dictador de Roma para defender la ciudad contra los ataques que sufría. Se le recuerda sobre todo por lo que hizo tras derrotar a los enemigos: inmediata y voluntariamente dejó el poder político y regresó a la vida campesina. Aclamado como «modelo de virtud cívica», Cincinnatus se ha convertido en un símbolo tanto del uso del poder político al servicio del interés público como del valor de limitar o incluso renunciar al poder individual por el bien de todos.

El e-mail empezaba así: «La seguridad de las comunicaciones de la gente es para mí muy importante», y su objetivo declarado era instarme a utilizar una codificación PGP para que él pudiera comunicarme cosas en las que, según decía, yo estaría sin duda interesado. Inventada en 1991, PGP, que significa *pretty good privacy* (privacidad muy buena), ha acabado convirtiéndose en una herramienta que protege de la vigilancia y los *hackers* el correo electrónico y otras formas de comunicación online.

En esencia, el programa envuelve los e-mails con un escudo protector, que es una contraseña compuesta por centenares, incluso miles, de números aleatorios y letras sensibles a las mayúsculas. Las agencias de inteligencia más avanzadas del mundo —entre las que sin duda se cuenta la NSA— poseen software de desciframiento de contraseñas capaz de hacer mil millones de conjeturas por segundo. No obstante, las contraseñas de la codificación PGP son tan largas y contingentes que el software más sofisticado necesita años para inutilizarlas. Quienes más temen el seguimiento de sus comunicaciones —como los agentes de inteligencia, los espías, los activistas de los derechos humanos o los *hackers*— confían en esta forma de encriptación para proteger sus mensajes.

En el e-mail, Cincinnatus decía que había buscado por todas partes mi «clave pública» de PGP, que permite intercambiar e-mail encriptado, y no la había encontrado. De ello había deducido que yo no estaba utilizando el programa: «Esto pone en peligro a todo aquel que se comunique contigo. No sugiero que deban estar encriptadas todas tus comunicaciones, pero al menos deberías procurar esta opción a los comunicantes».

A continuación, Cincinnatus hacía referencia al escándalo sexual del general David Petraeus, cuya aventura extraconyugal —que había puesto fin a su carrera— con la periodista Paula Broadwell salió a la luz después de que los investigadores encontraran en Google correos electrónicos entre los dos. Si Petraeus hubiera encriptado sus mensajes antes de enviarlos, escribía, o los hubiera almacenado en su carpeta de «borradores», los investigadores no habrían podido leerlos. «Encriptar es importante, y no solo para los espías o los mujeriegos». Codificar el e-mail, decía, «es una medida de seguridad fundamental para todo aquel que quiera comunicarse contigo».

Para impulsarme a seguir su consejo, añadía: «Por ahí hay personas de las que te gustaría saber cosas pero que

nunca establecerán contacto contigo si no están seguras de que sus mensajes no van a ser leídos durante la transmisión».

Luego se ofrecía a ayudarme a instalar el programa: «Si necesitas ayuda para esto, dímelo, por favor; si no, pídela en Twitter. Tienes muchos seguidores de gran competencia técnica dispuestos a brindarte asistencia inmediata». Por último, se despedía: «Gracias. C.»

Hacía tiempo que yo quería usar software de encriptación. Llevaba años escribiendo sobre WikiLeaks, los delatores de ilegalidades, el colectivo «hacktivista» conocido como Anonymous y temas afines, y también había establecido comunicación de vez en cuando con personas del *establishment* de la seguridad nacional de EE.UU., la mayoría de las cuales tiene mucho interés en la seguridad en sus comunicaciones y en evitar seguimientos no deseados. Por todo ello, el uso de software de codificación era algo que yo ya tenía en mente. Sin embargo, el programa es complicado, sobre todo para alguien como yo, poco ducho en programación y ordenadores. Era una de estas cosas para las que nunca encuentras el momento.

El e-mail de C. no me puso las pilas. Como soy bastante conocido por haber hecho la cobertura de historias que el resto de los medios suele pasar por alto, es mucha la gente que suele ofrecerme una «historia tremenda» que al final queda en nada. Y a menudo me encuentro trabajando en más casos de los que soy capaz de manejar. De modo que, si he de dejar lo que estoy haciendo para seguir una pista nueva, necesito algo concreto. Pese a la vaga alusión a las personas de las que me «gustaría saber cosas», en el e-mail de C. no había nada lo bastante tentador. No contesté.

Tres días después, volví a tener noticias de C., que me pedía la confirmación de que había recibido su correo. Esta vez respondí enseguida: «Lo recibí y voy a trabajar en ello. No tengo clave de PGP y tampoco sé cómo instalarla, pero buscaré a alguien que me ayude».