Marta Peirano

Entrevista a Edward Snowden

Su infancia son recuerdos de un Commodore 64 y del mundo infinito de los canales del IRC. Su adolescencia, la típica de un estudiante con inquietudes técnicas, afición por los Multijugadores Masivos y el resentimiento contra la autoridad. «Era demasiado guay para recurrir al vandalismo y no lo suficiente para drogarme. (…) En lugar de eso, empecé a hackear».

Sus habilidades le llevaron de los canales del IRC a la administración y el análisis de sistemas para las agencias de inteligencia más poderosas del mundo, sin sacarse un solo título universitario. Su conciencia le condujo a denunciar la existencia de la red de vigilancia más poderosa y peligrosa del mundo, y al exilio forzoso en Moscú, donde vive desde que EEUU le revocó el pasaporte en agosto de 2013. Su libro de memorias, *Vigilancia permanente*, se publica este martes 17 de septiembre en todos los países a la vez. Hablamos en exclusiva con el espía más famoso del mundo sobre sus memorias, el futuro de las comunicaciones y la posibilidad de reconstruir un sistema más justo con leyes, tecnología y el espíritu de resistencia de la comunidad.

En el libro hablas de los boletines, el IRC y esa atmósfera del Internet primigenio en el que un Snowden de 14 años podía aprender a construir un ordenador o a escribir código con la asistencia desinteresada de especialistas sin más ambición que la voluntad de aprender y la responsabilidad de contribuir a una comunidad técnica fuerte y preparada. ¿Podemos volver allí?

Ese momento es crucial. Porque, si recuerdas los primeros y mediados 90, sabes que había un sentido de comunidad, que estabas allí porque querías estar allí y era como eso que dicen de que hace falta todo un pueblo para educar a un niño. Los niños como yo éramos adoptados por adultos competentes en una especie de tutoría casual. Claro que había *flamewars* pero nadie se las tomaba en serio porque Internet no se tomaba en serio. Ahora no hay ese sentido de la comunidad ni ese sentido de responsabilidad. Los mayores odian a los jóvenes, los jóvenes desprecian a los mayores. *¡Millennial* es un insulto! La cuestión es, cómo recuperar ese sentido de la fraternidad cuando la tecnología ha dejado de conectar a las personas para animarlas a establecer su identidad en oposición a todo lo que no son.

El problema no es en la tecnología sino el objetivo de esa tecnología. La de ahora está diseñada para la explotación de los usuarios, no para incentivar la fraternidad. No hay ninguna razón por la que no podamos implementar redes distribuidas entre pares con otros objetivos.

Totalmente cierto, y es lo que estamos viendo en ciudades como Hong Kong. Otro de los grandes temas del libro son los Sistemas: sistemas políticos, sistemas legales, sistemas tecnológicos. Y, como dices, no es la tecnología lo que está fallando; la tecnología funciona bien. La cuestión es para quién trabaja. Lo que falla es el sistema, no la tecnología. Y lo que vemos es que, cuando la necesidad les empuja a escapar de ese sistema o tratar de reconstruirlo, es cuando surgen esas redes distribuidas, esas comunicaciones basadas en bluetooth y otras redes ad-hoc. Lo vemos una y otra vez en las manifestaciones porque ponen a la policía en una disyuntiva mucho más

compleja. Ya no pueden bloquear Signal o Telegram sino que tienen que bloquear todas las redes wifi, bloquear las antenas. Pero ya no pueden sabotear de manera selectiva a los usuarios de ciertas aplicaciones sino que tienen que cortar las comunicaciones para toda la población. Y hay gobiernos que no quieren hacer eso.

Cada vez hay más gobiernos dispuestos a cortar Internet.

Sí, pero mira, cuando Rusia trató de cortar Telegram porque no facilitaban las claves para descifrarlo –y que quede claro que no estoy recomendando en absoluto el uso de Telegram–, el Kremlin fue a su oficina de censura, Roskomnadzor, que es la agencia reguladora de comunicaciones del Estado, y les dijo que bloquearan Telegram. Pero Telegram estaba alojado en la nube de Google y en la nube de Amazon. Y Amazon los echa, pero Google no, y no pueden bloquear Telegram en Google sin bloquear la mitad de sus propias IPs. Al final consiguieron que los cientos de miles de empresas que dependían de los servicios de Google, incluyendo el propio gobierno ruso, se quedaran sin servicio –y sin taxis y sin comida a domicilio y sin pagos por móvil– porque todo está centralizado en los servidores de un par de gigantes tecnológicos. Una posición muy ventajosa si eres uno de esos dos gigantes o si eres uno de los gobiernos capaces de coaccionar o seducir a uno de esos gigantes para que haga lo que tú quieres.

Y muy mala si no eres ninguna de las dos cosas.

Si eres cualquier otro, es una posición muy vulnerable. Estamos construyendo vulnerabilidades sistémicas, concentrando nuestras comunicaciones, toda nuestra experiencia, en estos pocos gigantes. Cuando la web primigenia de la que hablábamos desapareció, esas empresas salieron en busca de un nuevo producto y ese producto fuimos nosotros. Y se colocaron oportunamente en medio de todas nuestras interacciones: cuando hablas con tu madre, cuando compras una pizza, cuando ves una serie, cuando sales a correr. Ellos están ahí, registrando todo lo que haces pero lo importante no eres tú sino todos nosotros. Y ahora que ya empiezan a tener el registro permanente de la vida privada de todos, ahora ellos tienen el control. Ya no somos colaboradores ni usuarios ni clientes. Somos su presa, sus súbditos, su material.

En el libro cuentas que te caíste del guindo cuando preparabas una charla sobre la red de vigilancia del Gobierno chino para la agencia. Te diste cuenta de que los chinos no estaban usando ninguna tecnología que los americanos no usaran también. ¿Cuál es la diferencia entre el sistema de crédito social chino y la red de vigilancia de EEUU, aparte de la visibilidad del primero y la opacidad del segundo?

China vigila abiertamente a sus ciudadanos y nosotros lo hacemos en secreto. Pero antes, al menos, podíamos decir que nosotros no encerrábamos a la gente en campos de concentración. Ahora mira lo que está pasando en nuestra frontera. O con la lista negra de terroristas, que solo ahora conocemos después de décadas de secuestros y operaciones secretas. Aún hoy, si estás en la lista no puedes saber por qué y por lo tanto no puedes defenderte para que te saquen de ella. En democracia, la visibilidad de las operaciones es lo que te permite defenderte de ellas. En China desgraciadamente no se puede resistir al estado. Pero en las democracias liberales, los gobiernos mantienen en secreto su red de vigilancia porque saben que generará el rechazo de la población. Y pueden hacerlo gracias a que las empresas privadas que facilitan esas redes de vigilancia pueden actuar con el mismo secreto, y la misma impunidad.

Hace poco vimos cómo Google y Facebook y Apple con Siri entregan nuestras conversaciones privadas a empresas externas y ninguno de los usuarios de sus servicios parecía saberlo. Una especialista como tú que estudia el fenómeno, que conoce la tecnología, puede intuir y deducir que la vigilancia de masas está ocurriendo, pero no lo puede demostrar. Y es esa chispa de distancia entre saberlo y poder demostrarlo es lo que lo cambia todo en una democracia. Porque, si no podemos estar de acuerdo en los hechos, no podemos tener un debate acerca de qué hacer al respecto.

¿Quién crees que es más peligroso, Donald Trump y el poder de su gobierno o Jeff Bezos, que aloja y procesa la mitad de Internet?

La gente diría Donald Trump, porque es evidentemente una persona horrible. Pero Trump no es el problema, sino el producto derivado de los errores del sistema. Pero la gente como Jeff Bezos sobrevive a los presidentes, no está sujeta a elecciones democráticas y tiene en sus manos el control de la infraestructura de todo el planeta. Es una amenaza completamente distinta. En Silicon Valley te dirán que Bezos no tiene un ejército, y es verdad. Pero Bezos no tiene un país ni necesita uno, porque tiene más dinero que muchos países.

¿Dirías que las grandes plataformas pueden competir con los estados nación?

De momento, los gobiernos tratan de beneficiarse del poder de estas empresas y las empresas entienden que se pueden beneficiar con menos regulación y la habilidad de influir directamente sobre la legislación, teniendo línea directa con presidentes, ministros, etc. Esta es la historia que cuentan los documentos PRISMA. Se pueden leer como un timeline: primero, cae uno; después, otro. El resto ven que la competencia lo hace y piensan oye, si ellos lo hacen y no hay consecuencia, nosotros lo hacemos también.

No piensas que vayan a dividir esos monopolios como hicieron con AT&T.

Los gobiernos obtienen su poder de esas empresas. ¿Cómo encuentran a la gente a la que quieren matar? El exdirector de la NSA, Michael Hayden, dijo literalmente: «matamos gente basándonos en metadatos». Sólo metadatos. Si creen que este teléfono pertenece a un terrorista, enviarán un misil contra la granja donde está localizado el teléfono, sin importar quién lo tiene en la mano porque lo que quieren es acabar con quien sea que usa ese teléfono y eso es peligroso. Es peligroso creer que puedes conocer a alguien, conocer sus planes, sus intenciones, su territorio; si son criminales, si son inocentes. Que puedes comprender a alguien así. Incluso si tienes acceso total a sus comunicaciones, la gente cambia de parecer, comete errores, miente incluso a las personas que más quiere. Nuestras comunicaciones no son el espejo de nuestra alma pero los gobiernos toman decisiones basadas en esos datos. Y así las justifican.

Y la legislación no evoluciona precisamente a favor de la privacidad.

Es 2019 y ya vemos lo que ocurre en Rusia, en China y en los EEUU. Pero incluso los países donde la vigilancia era ilegal de pronto la han legalizado después de un escándalo. Primero en Alemania [*Intelligence Service Act*, 2016], después en UK [*Investigatory Powers Act,* 2016] y lo mismo en Australia [*The Assistance and Access Act* 2018]. Y no dudo de que está pasando o pasará en España próximamente. La respuesta a los escándalos sobre vigilancia no ha sido

hacer que los servicios de inteligencia se ajusten a la ley, sino hacer que la ley se ajuste a los servicios de inteligencia.

Por otra parte, la cuarta enmienda en EEUU limita las capacidades del gobierno y del Estado pero no limita las de las empresas privadas. Este es un problema sistémico, un agujero estructural. Así que, cada vez que pienses en el poder de estos gobiernos, debes saber que proviene de los datos corporativos. Los gobiernos son peligrosos porque tienen acceso a todo lo que has puesto en el buscador de Google. Si no tienes una cuenta de Gmail, toda la gente que conoces tiene una y guarda copias de tus comunicaciones.

De hecho, ahora hay congresistas pidiendo que las empresas tecnológicas sean las que decidan sobre temas como la libertad de expresión.

Efectivamente, los gobiernos están empezando a delegar su autoridad a estas empresas, a convertirlos en pequeños sheriffs para que funcionen como agentes gubernamentales e impongan nuevas reglas, como qué se puede y no se puede decir y todo ese debate acerca del *«deplatforming»* [expulsar de la plataforma]. Se trata de una delegación de autoridad, voluntaria y deliberada, por parte de los gobiernos sobre estas empresas. Y lo que va a ocurrir, puede que no en dos años, pero en los próximos diez, cuando se den cuenta de que han ido demasiado lejos, es que no van a poder recuperar esa autoridad. Porque estas compañías habrán cambiado la manera en la que opera el sistema. Estas compañías opacas que no responden ante la ciudadanía habrán cambiado la manera en que la gente lee, come, conduce, trabaja, piensa y vota.

Una delegación de funciones que perjudica especialmente a los usuarios que ni siquiera son ciudadanos estadounidenses ni tienen derechos en esa legislación.

¡Exacto! ¿Cómo vais a controlar a Facebook en España, si ni siquiera os reconoce como una autoridad competente? El parlamento británico llama a Mark Zuckerberg a testificar y Mark les contesta «no sois lo bastante importantes para que yo vaya, voy a mandar a uno de mis agentes». Cuando ocurre algo así y no hay consecuencias, el precedente se extiende al resto de los CEOs de estas plataformas que dicen voy a pasarme un poco más de la raya a ver qué pasa. Y si los gobiernos han dejado de ser un mecanismo apropiado para expresar la voluntad de la ciudadanía, un instrumento para decidir el futuro de esa sociedad, qué es lo que nos queda. A dónde vamos.

Lo que vemos en Hong Kong, entre otros lugares, es una balcanización de la red a través de las plataformas: si quieres escapar del control chino, usas plataformas americanas; y si quieres escapar de las americanas, entonces usas plataformas rusas exiliadas en Berlín, como Telegram.

Lo que vemos en Hong Kong ya ha pasado antes: cuando nuestros modelos de autogobierno empiezan a fallar, inmediatamente pasamos al modo resuelveproblemas. Nos volvemos extremadamente utilitarios, fríamente pragmáticos y hacemos lo que tengamos que hacer para llegar a mañana, a pasado mañana y a la semana que viene, lo que haya que hacer para conseguir nuestros propósitos y seguir viviendo como queremos vivir. Y empezamos a elegir estas frágiles alianzas temporales sin darnos cuenta de que tienen un precio.

En Europa hemos optado por la GDPR, donde seguimos dependiendo de las plataformas pero interponemos una capa de legislación como medida profiláctica. ¿Es una estrategia

más realista?

La GDPR es significativa porque al menos demuestra una intención de cambiar esas estructuras torcidas. Pero no está siendo efectiva, ni lo será hasta que las plataformas paguen el 4% de sus beneficios en multas cada año, hasta que cambien de modelo. Y, de momento, ninguno de los comisionados europeos ha mostrado un verdadero interés por implementar esa solución. Quieren tratar a Facebook como un aliado. Facebook no es un aliado, no es un amigo. Apenas es un servicio realmente útil. Facebook es un depredador.

Facebook es la reencarnación de todos los errores que hemos cometido en nuestras políticas y leyes en los últimos 30 años. Es el fantasma que ha venido a atormentarnos. Y la manera de exorcizarlo es cambiando cosas. Cambiando la legislación, cambiando la tecnología, cambiando nuestras decisiones como consumidores y como ciudadanos. Es un cambio que no puede ocurrir en un solo nivel.

Y con una descentralización radical de las infraestructuras.

Uno de los motivos por los que tenemos este problema es que no hay espacio para la competencia. Las plataformas han diseñado sus servicios de tal manera que se han convertido en la autoridad central. Cualquiera que necesite métricas para ver cómo funciona su propia aplicación tiene que usar Firebase, la SDK de Google o Graph, la API de Facebook. Y toda la información de los usuarios de tu App pasa a ser de Google y de Facebook, sin que ellos lo sepan. Porque los usuarios no saben lo que es una SDK ni lo que es una API ni cómo funciona una App ni cómo funciona el teléfono. Solo saben apretar iconos. Tienes que ser un experto para saber usar estos dispositivos de manera segura. Y en el contexto de una autoridad central cada vez más corrupta, y de un estado de insatisfacción cada vez más patente y de una administración cada vez más incompetente, estas compañías han empezado a reemplazar a los gobiernos en pequeñas tareas administrativas. Como, por ejemplo, mantener bases de datos actualizadas de los ciudadanos, algo que hasta ahora era derecho único del estado.

O mantener datos biométricos de la población, algo que antes solo podía hacer la policía en casos justificados. ¿Cómo se resiste a esa clase de autoridad centralizada, corporativa, invisible y opaca?

Hay gente como Tim Berners Lee tratando de redescentralizar la red. Porque tenemos que cambiar la arquitectura de nuestras redes. Por ejemplo, tus lectores se habrán preguntado alguna vez por qué suena tu teléfono y ningún otro teléfono del mundo, cuando alguien te llama. ¿Cómo saben que eres tú? Por los identificadores únicos universales. Cada teléfono tiene al menos dos. Tienes el IMEI en el dispositivo, tienes tu IMSI en la tarjeta SIM y tu teléfono va gritando esos números al viento en todo momento, tan alto como lo permita el teléfono, hasta que la torre más cercana responde a la llamada, registra tu nombre y le dice al resto de la red que le pasen todas tus comunicaciones porque ahora estás en su jurisdicción. Y estos registros se guardan durante todo el tiempo que pueden.

Las operadoras en EEUU tienen registradas todas las llamadas que hemos hecho desde 1987. Y el de todos nuestros movimientos desde 2008. Cualquier operadora conoce los detalles de tu vida mejor que tú. La única manera de evitar estos registros es crear estructuras alternativas, sistemas alternativos, protocolos alternativos que no requieran una autoridad central. Que no requieran

confiar demasiado poder en las manos de unos pocos. Históricamente, cuando hay demasiado poder acumulándose en el garaje de alguien como Jeff Bezos, es solo cuestión de tiempo que lo use en su beneficio personal y en detrimento del bien común. Y eso no va a cambiar mientras tenga la oportunidad delante. La cuestión es cómo cierras esa oportunidad. No basta con cambiar a Jeff Bezos por otro, a Mark Zuckerberg por otro. Hace falta un cambio holístico, un cambio estructural.

Ahora mismo la fórmula mágica de las tecnológicas –ofrecer servicios gratuitos a cambio de datos– se expande a nuestras ciudades y gobiernos. El mismo Pedro Sánchez regresó de Bruselas hace unos meses celebrando un «acuerdo sin precedentes» con Amazon Web Services para mover la administración del Estado a la Nube de Amazon. Tampoco puedes tirar el móvil, abandonarlo todo y huir a las montañas porque tus identificadores únicos universales son tu cara y tu voz. Estas tecnologías están cada vez más diseñadas para controlar los movimientos de grandes masas de gente por todo el planeta, son los centinelas de un planeta al borde del desastre climático. ¿Tiene sentido seguir pensando en una Internet global descentralizada como Berners-Lee ¿No es mejor trabajar en miles de redes comunitarias locales, capaces de conectarse entre sí pero autosuficientes?

Los presidentes escogen a Amazon porque practican el culto de la eficiencia. Y esas formas de brutal sobreidentificación que mencionas, con esos identificadores biométricos que son indelebles, porque no se pueden cambiar –pero sí copiar, hackear, suplantar y duplicar–, presuponen que la identificación es buena porque optimiza la eficiencia. Habrás notado que el 80% de los países exigen ahora que te registres para poder tener un teléfono móvil. Que no haya un solo teléfono sin identificar.

El culto de la eficiencia significa que, si algo puede hacerse más rápido, por menos dinero y con menos esfuerzo, entonces es mejor. Todo el mundo está de acuerdo en eso. Pero si lees cualquier constitución de cualquier democracia liberal, como la de EEUU, verás que en nuestra Carta de derechos, cuatro de las principales enmiendas están diseñadas explícitamente para hacer que el trabajo del gobierno sea más difícil, menos eficiente. Y esto es lo que a menudo se olvida: la clase de dirigente que practica el culto de la eficiencia olvida que el exceso de eficiencia por parte del gobierno es una amenaza fundamental para la libertad de los ciudadanos.

Queremos que el trabajo de la policía, el trabajo de Hacienda, el trabajo de los publicitarios sea difícil, para que solo nos enfrentemos a esos grandes poderes cuando sea absolutamente necesario. Que el ejercicio de investigar la vida de una persona sea tan costoso, tan difícil, que solo se utilice cuando la alternativa sea impensable. Hace 30 años necesitabas un equipo coordinado de tres personas para vigilar a una sola persona. Hoy tienes una persona vigilando a poblaciones enteras. La única manera de evitar el abuso de poder es limitar la eficiencia de ese poder.

El 5G es el colmo de la eficiencia.

[Se ríe a carcajadas] Ya, ya. Cuando empezamos a hablar de la tecnología de ondas milimétricas [mWT] y de los puntos de acceso ultralocal que transmiten tu posición, no en el edificio ni en la habitación sino en una parte de la habitación, en un pasillo de la tienda, se me ponen los pelos de punta. No puede haber sino una ceguera ética completamente deliberada por parte de los responsables de este desarrollo. Hay una cosa: cuando en EEUU se han implementado este tipo

de tecnologías, se ha hecho pensando que éramos los únicos capaces de explotar sus vulnerabilidades, pero ahora vemos a nuestros vecinos y enemigos ponerse a la vanguardia. Por eso creo que veremos que el mundo de las redes y del software va a ser más seguro, más difícil de comprometer. Pero que, por otro lado, los gobiernos y compañías incluirán vulnerabilidades para su propia explotación, creando debilidades sistémicas que serán inevitablemente descubiertas por otros gobiernos, por otras empresas, por otros grupos organizados, con terribles consecuencias. Cuando eso pase, espero de todo corazón que tengamos redes locales ciudadanas.

España ha sido pionera en 5G con fibra de Vodafone y antenas de Huawei. ¿Qué te parece?

Sabemos a ciencia cierta que tanto los chinos, como los británicos usan su acceso a estas redes para perjudicar al resto del mundo. Este es el *status quo*, la naturaleza de un poder que ya conocemos hoy. Ahora, ¿cómo gestionas eso sin frenar el progreso? No es fácil. En el caso de 5G, tenemos un proceso en marcha que no sirve el interés público y tenemos una capacidad de producción que solo existe en un puñado de países, porque nuestras leyes de propiedad intelectual están tan rotas que incluso si un grupo de ingenieros españoles quisiera y supiera cómo implementar estas tecnologías, no tienen las patentes para fabricar los chips necesarios o las radios para producir estas transmisiones de manera independiente y segura. Todas las fábricas están en China o Taiwan, todas las patentes están en EEUU, China, UK o Noruega. Y EEUU tiene la información, porque el 80% del tráfico de contenidos pasa por EEUU. Las revelaciones de 2013 son el resultado directo de esa brutal asimetría en el acceso a la información.

No basta con cambiar gobiernos. Nada cambiará mientras vivamos en un mundo donde los chips solo pueden ser americanos o chinos, donde los métodos para fabricar radios que operan en cierta frecuencia tienen que estar licenciados y cumplir la legislación estadounidense o china, aunque vivas y trabajes en España, o Colombia o Chile. Donde la gente que ha creado el sistema en el que nos movemos siga colonizando los medios de producción, los medios de expresión.

Han convertido la propiedad intelectual en una herramienta de control político y social a escala global. Hasta que empecemos a mirar ese sistema y empezar a cambiarlo de manera que se puedan modificar estos aspectos fundamentales, la tendencia será la misma que hemos vivido hasta ahora: desempoderar a la ciudadanía para empoderar a las instituciones. Un concepto completamente antidemocrático.

Parece que la ventana de oportunidad existe, pero se está cerrando rápidamente.

Creo que estamos viendo la tensión de un mundo al límite, y que estamos al borde de algo y podemos caer en dos direcciones opuestas. Si caemos en la dirección correcta, habrá reforma. Si caemos en la mala, habrá revolución. Pero no podemos seguir como hasta ahora.

Estás en Rusia desde hace seis años porque tu gobierno te revocó el pasaporte, pero ibas camino de Ecuador. En vista de las actuales circunstancias, podemos decir que tuviste suerte.

Es una de esas ironías del destino. El gobierno de los EEUU trató de destruir mi vida exiliándome de forma permanente en un lugar donde soy un arma política, porque pueden desacreditarme sin

responderme, simplemente apuntando en el mapa. Pero puede que, con ese castigo, hayan salvado mi vida sin quererlo. Si ahora estuviera en Ecuador, bajo el mandato de Moreno y su desesperación por mostrar su lealtad a los EEUU, no es que crea que mi asilo hubiera sido revocado. Creo que probablemente estaría muerto o encarcelado, como Julian Assange.

Como director de la Freedom of the Press Foundation, qué futuro crees que le espera a este caso.

Creo que este caso se va a alargar durante años. Y creo que ha sido un error por parte de EEUU perseguir a un editor por publicar. Porque hay que tener claro que es eso de lo que ha sido acusado. No persiguen a Assange por ninguna de las numerosas polémicas que ha generado a lo largo de los años. Hay numerosas razones contra él. Pero los EEUU persiguen a Assange por el mejor trabajo que ha hecho Wikileaks. Y si dejamos que ganen, entonces nos merecemos el mundo que viene después.

[Fuente: *eldiario.es*]