REVISTA MEXICANA DE COMUNICACIÓN

NO. 146-147 / INVIERNO 2020-2021 / ISSN 2683-2631 / RESEÑA

Información en estados autoritarios: espionaje, perpetuidad y nula privacidad

Gustavo Rocha Reyes
UNIVERSIDAD AUTÓNOMA METROPOLITANA, UNIDAD CUAJIMALPA

Vigilancia permanente
Edward Snowden
México, Planeta, 2019.

En agosto de 2016, Marczak, B. y J. Scott-Railton publicaron para el Citizen Lab de la Universidad de Toronto: "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", un reporte que documentaba el uso del *malware* Pegasus contra el activista Ahmed Mansoor. Un dato que destacaba del mencionado reporte fue que México figuraba como el país que mayor participación presentaba respecto al aprovechamiento que dicha infraestructura dedicaba a suplantar la identidad de múltiples dominios en los que se enfatizaban las redes sociales, portales de noticias, sitios *web*, entre otros.

Tras el significativo hallazgo hubo dos organizaciones mexicanas dedicadas a la procuración de derechos digitales e investigación con perspectiva social: R3D (Red en Defensa de los Derechos Digitales) y Social TIC. Ambas profundizaron en los datos recabados por el equipo de investigación de Citizen Lab. En una operación conjunta que incluía a las organizaciones Access Now y Amnistía Internacional, realizaron el pedimento motivadas por la sospecha de que el *malware* Pegasus habría sido usado para espiar a ciertos activistas mexicanos defensores de la salud.

Lo que vendría después de estas revelaciones, sería un torrente de intentos para "infectar" con Pegasus los dispositivos de periodistas y defensores de derechos humanos en México. Este *malware* se conectaría a la infraestructura de Pegasus a través de mensajes de texto que contenían enlaces maliciosos.

Entre los casos de mayor relevancia documentados en *Gobierno Espía: vigilancia sistemática a periodistas y defensores de derechos humanos en México* destacan los siguientes: Centro de Derechos Humanos Miguel Agustín Pro Juárez, A.C. (Centro Prodh), Aristegui Noticias, Carlos Loret de Mola, Instituto Mexicano para la Competitividad (IMCO) y Mexicanos Contra la Corrupción y la Impunidad (MCCI).

En todos ellos, el común denominador era la delicada coyuntura política y/o los conflictos de intereses en los que cada uno de los actores se encontraba inmiscuido. En todos los casos se investigaban a diferentes sectores del gobierno mexicano. Uno de esos casos por ejemplo era la investigación que le realizaban al expresidente Enrique Peña Nieto, tanto por la casa blanca, como por la represión de San Salvador Atenco. Por lo anterior, podemos inferir cómo el gobierno mexicano infringió los límites de la vigilancia gubernamental y violó flagrantemente derechos humanos.

Ya en el 2013, Julian Assange, en su libro *Criptopunks: la libertad y el futuro del internet*, advertía de una amenaza muy severa para América Latina.

> El mundo debe ser consciente del riesgo que la vigilancia significa para América Latina y para el antiguo Tercer Mundo. La vigilancia estatal no solo es un problema para la democracia o para la gobernabilidad, sino que es un problema geopolítico. (…) Este es el nuevo juego: controlar la comunicación de miles de millones de personas y organizaciones. (…) La infraestructura de internet dirige gran parte del tráfico desde y hacia América Latina a través de cables de fibra óptica que físicamente atraviesan las fronteras de Estados Unidos. El gobierno de Estados Unidos no ha mostrado muchos escrúpulos en transgredir su propia ley al interceptar estas líneas para espiar a sus propios ciudadanos. Y no existen leyes que impidan espiar a ciudadanos extranjeros.
>
> Cada día cientos de millones de mensajes de toda América Latina son devorados por las agencias de espionaje de Estados Unidos y almacenados para siempre en depósitos del tamaño de ciudades. Los aspectos geográficos relativos a la infraestructura de internet, por lo tanto, tienen consecuencias para la independencia y soberanía de América Latina (2019: 10-11).

Los criptopunks abogan por el uso de la criptografía y otros métodos similares como medios para lograr el cambio social y político. El movimiento fue fundado a comienzos de la década de los noventa. Fue especialmente activo durante las “guerras criptográficas” de la década de los noventa y en la “primavera del internet” de 2011. Por su parte, Edward Snowden libraba una batalla personal para revelar el más grande secreto del gobierno estadounidense de la era actual: que recopilaba información privada de todo el mundo.

Snowden, en el presente libro, detalla su vida de forma notable, fluida y clara. Además, utiliza recursos de humor que aderezan el relato y muestran su extraordinaria capacidad intelectual. Snowden, por admirable que esto pueda parecer, deja siempre en segundo plano la faceta de tecnólogo que inherentemente representa y nos muestra una faceta lúcidamente humana.

Si bien ahora conocemos a Snowden como el sujeto que reveló algunos de los más grandes secretos de los servicios de inteligencia estadounidense, resulta curioso comprender cómo

se concebía él mismo desde sus más remotos pensamientos. Pues menciona que: "…desde que alcanzo a recordar, mi actividad favorita consistía en espiar".

No obstante, entender qué originó la afinidad tecnológica de Snowden es un tema aparte. Sus padres fueron trabajadores del gobierno de Estados Unidos y edificaron una identidad en torno del deber patrio. Su padre ocasionalmente llevaba a casa aparatos tecnológicamente avanzados para la época (década de 1990) porque eran costosos y difíciles de conseguir para las personas ordinarias. Estos aparatos despertaron los intereses del pequeño Edward por la informática. Su escuela fueron los videojuegos, mismos que obtenía mediante un sistema de canje por libros que sus padres diseñaron para que no se enajenara con la consola de NES (Nintendo Entertainment System).

Cuando Snowden tenía 9 años, se mudaron a Maryland, Carolina del Norte; más precisamente a Crofton, un lugar cercano a la Beltway, la carretera que rodea a la capital del país, en Washington D. C.. Desde aquel entonces, la autovía congregaba en sus barrios adyacentes a trabajadores del gobierno y a empresas que hacían negocios con él.

A los 12 años, con un ordenador que su padre había llevado a casa y una rudimentaria conexión a internet, Snowden convirtió a la red en "su santuario" o lo que él describió como "mi parque infantil, mi casa del árbol, mi fortaleza, mi aula sin paredes". La curiosidad que experimentaba por la apertura de un mundo virtual desconocido, se alimentaba de sus horas de sueño y poco a poco lo convirtió en una persona sedentaria.

Sus notas en el colegio disminuyeron a niveles alarmantes. Evidentemente era algo que había quedado en segundo plano. Internet ocupaba toda su atención y admiración:

> Me interesaba porque se trataba de gente entusiasmada. (…) internet fue en gran medida algo hecho de, por y para la gente. Su finalidad era ilustrar, no monetizar, y se administraba más bien con un conjunto provisional de normas colectivas en constante cambio que mediante contratos de condiciones de servicio explotadores y de aplicación global (68).

La nueva fascinación de Snowden se convirtió en manía. Ésta lo llevaría a descubrir la fragilidad de la seguridad informática. Tan pronto como pudo, recurrió al aprendizaje autodidacta y realizó su primer *hackeo*. Durante un recorrido por el directorio del sitio *web* de Los Alamos National Laboratory (un centro de investigación nuclear de Estados Unidos), logró vulnerar cierta información sensible. Cuando lo descubrieron era remarcable que alguien que ni siquiera había cumplido los 18 años hubiese sido capaz de realizar semejante acción. Para Snowden, ese fue el estímulo que lo convirtió en un sujeto de interés para el gobierno y, a su vez, que alimentó un profundo ego que satisfacía su neurosis tecnológica.

Su paso por el instituto fue la situación que cambió determinantemente su vida. Sus padres se divorciaron. A escasos meses de ingresar, le diagnosticaron mononucleosis infecciosa. Debido a la enfermedad, abandonó la secundaria y mermaron sus esperanzas de ingresar a la universidad. Sin embargo, encontró una salida cuando supo que la Anne Arundel Community College (AACC), una universidad acreditada no tan venerable, lo aceptaría sin el título de secundaria.

Con una enfermedad que prácticamente lo invalidaba, el AACC implicaba la dificultad de acudir dos veces por semana a un campus situado a veinticinco minutos de su casa en automóvil. Era el estudiante más joven de la universidad; situación que lo convirtió en una excentricidad. En un esfuerzo máximo y antes de cumplir los dieciséis años, realizó el último examen en el Estado de Maryland que le concedió un título de General Education Development que equivalía al certificado de secundaria.

El 11 de septiembre fue un día que marcaría toda una época. En esos momentos Snowden trabajaba como diseñador *web* para la empresa de una de sus amigas de la universidad. Tras los atentados, entendió que "…Estados Unidos [había dividido] al mundo en «nosotros» y «ellos», y toda la gente estaba con «nosotros» o contra «nosotros»…" (115) por lo que sintió la necesidad de hacer algo por su país.

Todos sus conocidos habían trabajado para el gobierno. Si bien hasta ese momento había sido cauteloso de no trabajar para la administración del país Estados Unidos se iba a guerra y él quiso ser parte de ello hacer algo por su nación. Decidió enlistarse en el ejército: "De lo que más me arrepiento en la vida es de mi apoyo reflexivo e incondicional a esa decisión" (116).

Después vivió una vertiginosa carrera asociada a la Intelligence Community (IC). Tras una serie de eventos desafortunados y una sucesión de casualidades obtuvo la habilitación TS/SCI (Top Secret/Sensitive Compartmented Information). Se trataba de la certificación más alta respecto a la capacidad de manejar información secreta del gobierno estadounidense.

Snowden descubrió los secretos que paralizaron al mundo mientras dedicaba su vida a la IC en edificios de alta seguridad con paradero reservado. La NSA (National Security Agency) utilizaba, mediante legislaciones resueltas a modo, dos métodos de vigilancia por internet conocidos como PRISM y Upstream:

> PRISM permitía a la NSA recopilar de forma rutinaria datos de Microsoft, Yahoo!, Google, Facebook, PalTalk, YouTube, Skype, AOL y Apple, lo que incluía *emails*, fotos, conversaciones de vídeo y audio, contenido de navegación *web*, consultas en motores de búsqueda y todos los demás datos almacenados en sus nubes, de forma que las empresas se convertían en co-conspiradoras conscientes. Por su parte la recopilación Upstream era un método sin duda más invasivo: permitía recoger datos rutinaria y directamente de la infraestructura de internet del

> sector privado, eso es, de los conmutadores y enrutadores que derivan el tráfico de internet en todo el mundo. […] Juntos PRISM (recopilación de datos en los servidores de grandes proveedores de servicios) y la recopilación Upstream (recogida directa de la infraestructura de internet), garantizaban la posibilidad de someter a vigilancia la información de todo el planeta, estuviese almacenada o en tránsito (300-301).

Al saber esto, Edward Snowden consideró hacer una denuncia del espionaje que el gobierno estadounidense ejecutaba sin consentimiento; es más, sin el más mínimo escrúpulo. Cualquier coartada era suficiente para que significase un potencial riesgo jurídico para el gobierno:

> "[…] el archivo más famoso de los que desvelé, [fue] una diapositiva de una presentación en Power Point de 2011 que describía la nueva postura de la NSA en materia de vigilancia como una cuestión de seis protocolos: «Husmea en todo, Entérate de todo, Recógelo todo, Procésalo todo, Aprovéchalo todo»" (299).

Para Snowden resultaba inconcebible que fuésemos "(…) las primeras personas en la historia del planeta (…) que llevan a sus espaldas la carga de la inmortalidad de los datos (…)" (436).

A través de la criptografía, Julian Assange ha buscado, por ejemplo, lograr un cambio social y político en el mundo. De la misma forma, Edward Snowden describe en estas páginas las andanzas que tuvo que sufrir al revelar los secretos del país más influyente del mundo. Una apuesta que pagó con la pérdida de la libertad en beneficio de la privacidad de las personas.

> Este es el resultado de dos décadas de innovación sin supervisión ninguna, el producto final de una clase política y profesional que sueña con ser nuestra dueña y señora. Da igual el lugar, da igual el momento, y da igual lo que hagas: tu vida se ha convertido en un libro abierto (428).

Fuentes

- Article 19, R3D (Red en Defensa de los Derechos Digitales) y Social TIC. (2017). *Gobierno Espía: vigilancia sistemática a periodistas y defensores de derechos humanos en México*. Creative Commons.
- Assange, J. (2013). *Criptopunks: la libertad y el futuro del internet.* Buenos Aires: Marea; Trilce.
- Snowden, E. (2019). *Vigilancia Permanente*. México: Editorial Planeta Mexicana.

REVISTA MEXICANA DE COMUNICACIÓN

NO. 146-147 / INVIERNO 2020-2021 / ISSN 2683-2631 / RESEÑA