“Ninguna democracia se puede permitir tener herramientas tan poderosas como Pegasus”

Por: Sebastiaan Faber. 03/06/2022

Pegasus acaba de remover las aguas políticas españolas, pero la verdad es que lleva años cabalgando. En 2017, por ejemplo, la mexicana Red en Defensa de los Derechos Digitales (R3D) publicó un informe que demostraba cómo dos gobiernos mexicanos habían usado el notorio software del grupo NSO para espiar a periodistas, activistas, políticos y defensores de derechos humanos al menos desde 2015. Solo en México, donde los primeros contratos de agencias gubernamentales con NSO datan de 2011, se han llegado a identificar hasta 15.000 teléfonos infectados.

Fundada en 2014, R3D defiende el derecho a la privacidad en la comunicación digital, el acceso universal al internet de banda ancha, la libertad de expresión digital y el conocimiento libre. Luis Fernando García, director ejecutivo de la Red desde sus inicios, es licenciado en Derecho y máster en Derechos Humanos.

Ustedes llevan mucho tiempo advirtiendo contra los peligros de programas como Pegasus. ¿Cuánto hay de nuevo en el informe de Citizen Lab y el reportaje del *New Yorker* sobre la vigilancia a independentistas catalanes y vascos que tanto revuelo ha causado en España?

Desafortunadamente la historia es muy similar a las que conocemos no solo de México sino de otras partes del mundo, desde países decididamente autoritarios como Arabia Saudí y democracias débiles como México a democracias con un prestigio mayor, como la española.

¿Esa ubicuidad, qué indica?

Nos habla de que tal vez el problema no sea el tipo de Estado o su organización democrática, sino el tipo de herramientas que se está usando.


ctxt
TALLER EN LÍNEA
Próximos
talleres en línea
que no te puedes
perder
APÚNTATE
Información: info@ctxt.es

¿Ve diferencias entre lo que ha venido ocurriendo en España y lo que pasó en México?

Hay paralelismos y divergencias. En México, donde llevamos unos cinco años desde las primeras denuncias sobre el uso de Pegasus, prácticamente no ha pasado nada. No ha habido apenas un proceso de esclarecimiento. Nadie ha asumido responsabilidades. El gobierno se enrocó en la negación. En España, en cambio, el Gobierno optó por reconocer el espionaje y defenderlo. Eso, la verdad, me sorprendió. ¿Cómo se puede defender políticamente el espionaje a diputados, que encima son aliados de tu gobierno? Además, el hecho de que el Gobierno español defendiera que las escuchas se hicieron con autorización judicial lleva a pensar que hay un problema con el Poder Judicial, que al parecer está dispuesto a autorizar ese tipo de intervenciones. Eso sí, a diferencia de lo ocurrido en México, en España sí que ha habido al menos un cese, aunque parece que no fue por el espionaje interno, sino por el fallo a la hora de defender al Gobierno del Estado de ataques de otros gobiernos.

Algunos han alegado que los Estados siempre espían. Si antes se escondían micros, pinchaban teléfonos y abrían sobres, hoy los servicios secretos hurgan en los móviles. En otras palabras, han cambiado los métodos, pero el principio es el mismo.

Que no sea nuevo no lo justifica de ninguna manera. Pero además es importante entender la diferencia entre lo que se hacía antes y lo que ocurre hoy, dada la potencia de las herramientas que se están usando y la cantidad de información que generamos como personas en contacto con distintos dispositivos digitales. No es lo mismo una intervención de comunicaciones de los años 80 que un programa como Pegasus, que da acceso no solo a llamadas, sino a mensajes, fotografías, contactos, archivos, todo lo que teclees, la cámara, el micrófono, la geolocalización, en un dispositivo que nos acompaña a todos lados y que abarca nuestra vida entera. Es una vigilancia mucho más intensa que la de antes.

> No es lo mismo una intervención de comunicaciones de los años 80 que un programa como Pegasus

¿Qué significa esto en términos de derechos humanos?

Significa que, si ya antes la vigilancia estatal era cuestionable, hoy lo debería ser mucho más. Significa que nos toca repensar y replantear la legitimidad de las actividades del Estado en una democracia. Hace falta modificar radicalmente lo que consideramos aceptable. ¿Dónde están los límites de la vigilancia? ¿Qué mecanismos y funciones son necesarios para controlar ese poder? El tipo de vigilancia que pueden ejercer los Estados hoy no tiene nada que ver con el de antes, ni las consecuencias son las mismas.

¿Las consecuencias?

Los efectos concretos de estas prácticas a lo mejor se pueden trivializar en un país como España. Pero en otras partes son muy, muy graves. En México –donde son asesinados más periodistas que en muchos países en guerra–, el espionaje ha tenido como objetivo a periodistas, a defensores de derechos humanos, a los familiares de los 43 desaparecidos en Ayotzinapa, así como a sus abogados y el grupo de expertos independientes que fue invitado al país a ayudar con la investigación.

> Nos toca repensar y replantear la legitimidad de las actividades del Estado en una democracia

Ayotzinapa ha vuelto a poner el foco en la connivencia entre el Estado mexicano, sus fuerzas de seguridad y el crimen organizado.

Es verdad que en México no siempre hay una línea bien definida entre Estado y delincuencia. Pero lo mismo sucede en todas partes, España incluida: no hay Estado sin elementos corruptos. Ahora bien, ya hemos visto cómo se ha abusado de herramientas como Pegasus en países autoritarios como Arabia Saudí. Pero sería un grave error aceptar o normalizar su uso en países con una tradición democrática más consolidada. Por más sólidas que sean las instituciones democráticas de un país, este puede acabar avasallado por el poder del dinero, del crimen o del fascismo. Recordemos lo ocurrido en Polonia o Hungría. Ninguna democracia se puede permitir tener una caja negra tan poderosa que opera con tan pocos controles y que resulta tan fácil de abusar de maneras terribles.

Otra diferencia con la vigilancia estatal de antes es el papel central que juegan hoy las empresas privadas, incluidas empresas con fuertes vínculos estatales

como lo es el Grupo NSO.

Hay numerosos Estados que tienen una capacidad tecnológica suficiente para desarrollar sus propias herramientas de vigilancia o que han generado y apoyado poderosas industrias. Israel no es el único, ni mucho menos. También hay herramientas italianas, estadounidenses, británicas, alemanas y chinas que están empezando a aparecer. Además, se trata de programas cada vez más avanzados. En los casos que inicialmente detectamos en México, por ejemplo, era necesario darle clic a un enlace para activar el programa. Hoy ya no es necesario que el usuario haga nada para que se infecte su dispositivo. Es difícil exagerar la gravedad del asunto. No olvidemos que este tipo de tecnología depende de la explotación de vulnerabilidades en software y hardware que utilizamos miles de millones de personas en el mundo.

> Por sólidas que sean las instituciones democráticas, pueden caer ante el poder del dinero, del crimen o del fascismo

Vulnerabilidades que las empresas tecnológicas y los Estados dicen querer subsanar.

Bueno, hasta cierto punto. Por un lado, hay todo un discurso global sobre la ciberseguridad y sobre el hecho de que nuestra sociedad y economía dependen cada vez más de la resiliencia de los dispositivos electrónicos en los que están basados nuestros trabajos, nuestras vidas personales, nuestras industrias, etcétera. Pero al mismo tiempo, esos mismos Estados, incluidas muchas democracias, están incentivando lo que esencialmente es una industria de criminales informáticos enfocados en identificar vulnerabilidades, no para reportarlas y que sean parcheadas, sino para explotarlas con fines de ganancia personal.

No deja de ser una actitud hipócrita de parte de los Estados.

Pero además es irresponsable porque amenaza la seguridad de miles de personas. Hay un montón de ejemplos de herramientas de vigilancia desarrolladas por gobiernos que terminan siendo utilizadas para fines criminales. Eso pasó en Estados Unidos, donde se robaron herramientas de la NSA que después fueron usadas por hackers norcoreanos y chinos –delincuentes informáticos– en contra de las propias industrias estadounidenses.

Desde R3D, ustedes abogan por un cambio fundamental de actitud.

El mundo tiene que tomar decisiones que no ha querido tomar. Tenemos que elegir qué queremos. ¿Queremos que nuestra estructura tecnológica, cada vez más importante para la vida moderna y para la economía y para la sociedad, sea resiliente y segura? ¿O queremos que no sea resiliente y segura para así poder seguir espiando a las personas? Es un dilema de seguridad que no se ha querido afrontar. En cambio, se ha querido generar ambigüedad para que algunos Estados exploten esas vulnerabilidades informáticas.

> Son muchas las herramientas de vigilancia desarrolladas por gobiernos que terminan siendo utilizadas para fines criminales

Argumentan ustedes que la industria del espionaje también explota las vulnerabilidades de los propios Estados. Si un programa como Pegasus se cuela por la puerta trasera de una aplicación, empresas como NSO acaban por colarse en las instituciones, corrompiéndolas.

La industria de la vigilancia genera problemas no solo de seguridad sino políticos, morales y jurídicos. En México hemos visto claramente que las compras de herramientas de espionaje son fuentes importantísimas de corrupción. Como se trata de contratos secretos por razones de seguridad nacional, les rodea una opacidad y una discrecionalidad muy propicias para inflar precios, elegir proveedores, encajar mordidas indebidas… ¡Todo del gasto público! Sabemos, además, que países como Israel utilizan esas ventas también como una herramienta diplomática. Lo que no sabemos es si, después, de alguna manera tienen acceso a la inteligencia que genere el uso del software de vigilancia por los clientes.. La opacidad es total.

Ustedes, en cambio, piden transparencia.

Si los Estados nos piden que aceptemos la vigilancia como un mal necesario, tienen que aceptar que sepamos mucho más sobre qué poder tienen y cómo lo utilizan. ¿Van a ser menos efectivas sus herramientas con más transparencia? Puede ser. Pero en el caso contrario, el riesgo es demasiado grande, como ya hemos visto.

> Si nos piden que aceptemos la vigilancia como un mal necesario, tenemos que saber mucho más sobre qué poder tienen

¿Cuáles son los agentes o agencias mejor situados para asegurar esa transparencia? ¿Quién debería ejercer el control que hoy falta? ¿La judicatura?

El control judicial es importante, pero no es suficiente. El mismo caso de España ejemplifica que el control judicial no necesariamente garantiza que estas herramientas vayan a ser utilizadas de manera adecuada. Más importante que el control judicial es la *regulación* de este tipo de herramientas: qué puede adquirirse y usarse. Tenemos que asumir que no toda herramienta es legítima. Algunas simplemente conllevan demasiado riesgo. Hay que comprender que una democracia simplemente no resiste que alguien dentro del Estado tenga acceso a una herramienta tan poderosa, por más útil que pueda parecer. No todo lo que es útil es necesariamente compatible con una democracia. Este es el debate que tenemos pendiente.

¿Y después del debate?

Es importante generar mecanismos institucionales capaces de prevenir o evitar los abusos. Esto significa, en primer lugar, que debe ser posible *detectar* esos abusos. Uno de los problemas principales de este tipo de violaciones de derechos humanos es la dificultad de su detección. Las víctimas muchas veces no son conscientes de serlo. Ni mucho menos se dan cuenta de las formas en que el espionaje está afectando su vida. Las consecuencias pueden ser muchas y muy graves, como hemos visto en México. Van desde la extorsión, el chantaje y los ataques reputacionales hasta los ataques físicos y legales o incluso la muerte. Ha habido casos de periodistas espiados que acabaron asesinados. La dificultad de la detección hace que los que te espían puedan joderte la vida sin que te des cuenta.

Y aunque te acabes dando cuenta no lo puedes demostrar.

Exacto. Mira, no estoy diciendo que el espionaje digital sea una violación de derechos humanos más grave o importante que otras violaciones, como la tortura o el asesinato. Pero al menos, cuando te torturan, sabes que estás siendo torturado. Se genera evidencia en tu cuerpo. Es una violación que las herramientas tradicionales de defensa de derechos humanos están más capacitadas para documentar. En el caso de Pegasus y programas similares estamos tratando de documentar lo invisible, lo secreto, lo difícil o imposible de detectar. Esa misma invisibilidad también hace que a la sociedad le cueste asumir la seriedad del asunto. Por eso las organizaciones alrededor del mundo que nos dedicamos a este tema tenemos como principal objetivo tratar de sacar a la luz cosas que están escondidas y evidenciar las gravísimas consecuencias de estas violaciones de derechos humanos. En México y en muchas partes del mundo, vigilar ilegalmente es un delito muy grave. ¿Pero de qué sirve que se penalice con muchos años de cárcel si no tengo manera de saber quién espía a quién? Por eso, precisamente, hay que crear mecanismos no solo para evitar o prevenir que los abusos sucedan, sino para que, si suceden los abusos, se puedan detectar.

Esta lucha por la transparencia exigirá un cambio importante en la cultura política.

En parte estamos enfrentándonos a un círculo vicioso. En México, particularmente, la vigilancia ha sido una herramienta fundamental para mantener los pactos de impunidad entre las clases políticas y económicas, pero también entre éstas y el crimen organizado. El espionaje mutuo fomenta las complicidades y la extorsión.

Esto a su vez genera acuerdos para mantener todo bajo el agua, lo que solo hace que se puedan perpetuar este tipo de abusos sin que nadie le ponga un freno.

En fin, los obstáculos son muchos.

Definitivamente. Para empezar, hay una asimetría de poder muy importante. Pero creo que lo que se ha logrado en los últimos años, en lo que hemos sacado a la luz este tipo de casos, ha generado oportunidades únicas, históricas, que tampoco van a ser para siempre. Hay que aprovecharlas ya. No hay tiempo que perder. La tecnología va a seguir avanzando, va a ser cada vez más poderosa y menos detectable. Quienes tienen acceso a este gran poder van a seguir encumbrándose en el poder político y económico, minando las luchas democráticas.

A pesar de todo, le detecto cierto optimismo.

El trabajo que hemos hecho está surtiendo efecto. Ha detonado, por ejemplo, que compañías como Facebook, WhatsApp o Apple demanden a NSO. Y eso sin duda ayuda a la correlación de fuerzas. Por otra parte, sigue habiendo relaciones de complicidad entre Estados e industrias –incluidas, desde luego, las grandes empresas tecnológicas como Facebook y Apple, cuya colección y uso de datos personales también se tiene que controlar más– que hay que empezar a romper. Por otra parte, hay cada vez más conciencia de que las herramientas de vigilancia de origen chino, israelí, estadounidense, etcétera pueden representar una amenaza a la seguridad nacional de los países que las compren. Creo que cada vez más países se preguntarán si quieren depender de determinadas herramientas –por más poderosas, útiles o atractivas que puedan parecer– sin saber a quiénes benefician realmente.

Entonces, sí, yo creo que ha habido muchos avances. Los organismos internacionales de derechos humanos han empezado a involucrarse más. Se habla de moratorias a la industria de la vigilancia. Y se han abierto debates sobre los marcos jurídicos para la utilización de estas herramientas y la rendición de cuentas. Pero como decía, no sé cuánto va a durar esta oportunidad. Hay que actuar ya. Tenemos que seguir visibilizando los efectos de estas invasiones de la privacidad y demostrar cómo pueden minar las libertades democráticas y ser utilizadas para fines de opresión política. Tenemos que movilizarnos. En el fondo, esta es una disputa política, jurídica, económica y cultural. Los abusos están pasando, no hay duda. Pero no son inevitables. Es necesario –y posible– desarrollar soluciones prácticas y

reales.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: CTXT

Fecha de creación
2022/06/03