Casos: *Wikileaks,* Snowden y ahora México

*Alberto E. Nava Garcés**

Sumario: I. Introducción **II.** La ciberseguridad en México es un tema grave **III.** *Wikileaks* **IV.** El caso Snowden **V.** Las nuevas tecnologías de la información, la comunicación y el derecho penal **VI.** El caso mexicano

Resumen: En la actualidad se han visualizado distintas conductas delictivas que han puesto en estado crítico a diversos Estados, en algunos casos los gobernados han celebrado que esta información se publique, sin embargo, lo anterior solo visibiliza lo débil del sistema gubernamental.

Abstract: In present times, different criminal behaviors have been visualized that have put various States in a critical status; in some cases, citizens have celebrated that this information is published. The above, however, only exposes the governmental system's various weaknesses.

Palabras clave: Ciberseguridad, Hackeo, *Wikileaks*, Snowden, SEDENA.

Key words: Cibersecurity, Hacking, *Wikileaks*, Snowden, SEDENA (México)

I. INTRODUCCIÓN

Tenemos que partir, como lo hemos escrito en ocasiones anteriores que el uso indebido de la tecnología solo se puede combatir (y prevenir) con tecnología. En el caso que presentamos, es evidente que falló o fue inexistente la tecnología para evitar la filtración de información y más pronto veremos hasta donde nuestra precaria legislación puede dar respuesta a un problema de cualidades especiales donde se confronta la libertad de prensa, el derecho a la información contra lo que pudiera ser una auténtica confidencialidad de la información gubernamental o la opacidad de un gobierno para dar a conocer cuestiones que deberían ser del interés de la sociedad.

El 29 de septiembre de 2022 se dio a conocer que la Secretaría de la Defensa Nacional (SEDENA) había sido hackeada y, el tamaño de la información sustraída

* Miembro de número de la Academia Mexicana de Ciencias Penales.

es aproximadamente de seis terabytes, lo cual habla de una ingente cantidad de documentos confidenciales de toda índole no testados: contratos, estado de salud del presidente, destacamentos, estrategias, comunicaciones y se dice que hasta documentos de inteligencia que contienen seguimiento e intervención de comunicaciones.

Se trata de una de las instituciones más herméticas del Estado Mexicano y la cual ha ido aumentando sus responsabilidades en los últimos 15 años, entre las que se incluye todo un aparato de inteligencia para tener el control de las comunicaciones de este país. Con lo días sabremos hasta dónde llega esta, debido a la cantidad de información que, se dice, fue sustraída.[1]

---

1 "Hackers rompen seguridad digital de Sedena; extraen miles de documentos, revela Loret"
El grupo de hackers, autodenominados 'Guacamaya' sacó a la luz registros de la salud de AMLO, la orden para liberar a Ovidio Guzmán y diferendos entre las cabezas de la Marina y la Defensa Nacional
El grupo de hackers, autodenominados 'Guacamaya', accedió a información de la Sedena y logró un hackeo masivo que sacó a la luz algunos de los más polémicos asuntos de seguridad que ha enfrentado esta administración.
La información recabada la hicieron llegar al periodista Carlos Loret de Mola, quien en su espacio informativo Latinus dio a conocer la información esta noche, especialmente los registros de la salud del presidente López Obrador, y lo que sería un ocultamiento de un traslado en calidad de 'grave' del mandatario.
'El 2 de enero de este año, una ambulancia aérea del Ejército tuvo que ir a Palenque, Chiapas, donde se encuentra el rancho del presidente López Obrador, para trasladarlo al Hospital Central Militar de la CDMX.
Una serie de documentos confidenciales revelan que ese día, en Palenque, el presidente tuvo que ser monitoreado, canalizado y medicado antes de volar al aeropuerto de la Ciudad de México, desde donde fue llevado de inmediato, en helicóptero, al hospital militar con diagnóstico grave', dice Loret en su programa de Latinus.
A López Obrador se le diagnosticó con angina inestable de riesgo alto, un preocupante mal cardiaco que puede conducir a infartos. Luego del 2 de enero, en Palacio Nacional, se le tomaron muestras de sangre y de laboratorio, una semana después, el día 10, López Obrador anunció en Twitter que tenía Covid-19… Ni él ni nadie de su gobierno se refirió al traslado de emergencia ni al diagnóstico grave…
El Culiacanazo
Uno de los documentos revelan cómo los hijos del Chapo Guzmán 'doblaron' al gobierno mexicano en el operativo conocido como Culiacanazo, ocurrido el 17 de octubre del 2019.
En uno de los correos revisados se pone como ejemplo un parte especial del Culiacanazo para que los militares de la Guardia Nacional redacten así este tipo de informes. En el documento se hace un resumen de lo sucedido:
'El Ejército establece que a las 15 horas con 15 minutos 'se llevó a cabo la detención de Ovidio Guzmán, cumplimentando una orden de aprehensión girada el 2 de abril de 2018 por la Corte Federal de Columbia en Estados Unidos, por los delitos de delincuencia organizada con la finalidad de acopio y tráfico de armas, secuestro, cobro de piso y delitos contra la salud'.
'El parte militar explica que dos minutos después, 'los efectivos de seguridad invitan a Ovidio a persuadir a sus hermanos de cesar su actitud hostil', y que para ello se comunicó directamente con 'Iván Archivaldo Guzmán Salazar, conminándolo a ordenar el cese de las agresiones, pero su hermano respondió con una negativa y lanzó amenazas contra el personal militar y sus familias".

Con un tema de este calado aparecen varios subtemas: ¿hasta dónde puede llegar la libertad de prensa, garantizada por nuestra Ley Fundamental? ¿La tecnología abre un boquete en las instituciones? ¿Hay un bien jurídico tutelado en la información confidencial? y ¿Qué dicen las leyes al respecto?

II. LA CIBERSEGURIDAD EN MÉXICO ES UN TEMA GRAVE

La reciente filtración nos coloca entre los casos de Wikileaks, Snowden y supera por mucho lo ocurrido con el caso Pegasus cuyos resultados apenas hemos podido vislumbrar en los últimos meses, sin que haya responsabilidades claras al respecto. Aun si los documentos obtenidos a la SEDENA (Secretaría de la Defensa Nacional) no tuviesen información de carácter ilícito, la sola información estratégica y las comunicaciones revelan un tema que ya no puede postergarse. ¿Hubo hackeo u obtención desde adentro de las instituciones?

El gobierno mexicano, a través del titular del Ejecutivo ha hecho una defensa pública de lo que en su momento hiciera Julian Assange sobre revelaciones de información clasificada de distintos gobiernos, el llamado caso Wikileakes, ahora que el ejército lo ha padecido, cabe preguntarse ¿Seguirá el gobierno defendiendo las revelaciones de Assange? ¿Seguirá convencido de que esto puede quedar impune?

Por lo anterior, transcurridas algunas horas, el presidente Andrés Manuel López Obrador 'dobló las manos ante el cártel de Sinaloa', señala la pieza de Loret en Latinus.

El parte militar señala: 'A las 19:30 horas, se recibe la orden por parte del Ciudadano Presidente de la República del cese del operativo para detener a Ovidio Guzmán López'.

Otro punto a destacar es que la versión oficial sobre las víctimas mortales del Culiacanazo menciona que fueron ocho; no obstante, los documentos internos de las Fuerzas Armadas señalan que se fueron nueve personas fallecidas.

Ojeda y Cresencio, 'un choque'

Un dato más que revela Latinus es que hay una carta del secretario de Marina, almirante Rafael Ojeda, al secretario de la Defensa, general Luis Crescencio Sandoval, en el cual muestran sus diferencias sobre la seguridad en el Aeropuerto Internacional de la Ciudad de México (AICM), con fecha del 22 de junio pasado.

En uno de los párrafos escritos por el almirante Ojeda se puede leer lo siguiente:

'Esto no es cuestión de números, sino de coordinación entre instituciones, siempre respetando nuestras áreas de competencia… nunca con la intención de buscar protagonismos'.

Carencia del Ejército en cruces fronterizos

Otro dato de seguridad nacional que dieron a conocer es cuánto personal del Ejército está destacamentado en cada uno de los cruces fronterizos de Tijuana, y en cada punto táctico.

Destacan que, en la frontera sur, en Cancún, el caso es 'especialmente grave', según la nota de Latinus, pues en el terminal e del aeropuerto de Cancún la Defensa admite que lo óptimo es contar con 56 elementos y solo hay 14.

En algunos horarios, la presencia de personal es de 3 militares, lo cual pone a esta zona en 'condiciones de debilidad críticas", que dejaría una puerta abierta para todo tipo de tráfico ilegal.

apr/ml Consultado en: https://www.eluniversal.com.mx/nacion/hackers-rompen-seguridad-digital-de-sedena-extraen-miles-de-documentos-revela-loret el 29 de septiembre de 2022, 22:00 hs.

III. *WIKILEAKS*

En el año 2010 se hizo famoso el nombre de Julian Assange, fundador y director de *Wikileaks*, pues utilizó la red para dar a conocer documentos relacionados con la invasión norteamericana a Afganistán y más tarde documentos relativos a la guerra entre Estados Unidos de América e Irak. Sin embargo, meses más tarde *Wikileaks* realizaría algo inédito: realizar la filtración de documentos secretos emitidos por la diplomacia de los propios Estados Unidos.

La información fue enviada a cinco periódicos para que de manera paulatina fueran ministrando la información: *El País* (España), *Le Monde* (Francia), *Guardian* (Reino Unido), *New York Times* (Estados Unidos de América) y *Der Spiegel* (Alemania). Estos cinco diarios revelaron el contenido de la mayor filtración de documentos secretos a la que jamás se haya tenido acceso en toda la Historia. Se trata de una colección de más de 250,000 mensajes del Departamento de Estado de Estados Unidos, en los que se descubren episodios inéditos ocurridos en los puntos más conflictivos del mundo, así como otros muchos sucesos y datos de gran relevancia que desnudan por completo la política exterior norteamericana, sacan a la luz sus mecanismos y sus fuentes, dejan en evidencia sus debilidades y obsesiones y, en conjunto, facilitan la comprensión por parte de los ciudadanos de las circunstancias en las que se desarrolla el lado oscuro de las relaciones internacionales.[2]

El ciudadano común pudo enterarse de cómo se manejan los hilos de la política doméstica desde Washington. Promoción de leyes, investigación de vidas privadas, estados de salud (y de ánimo) de gobernantes se pudieron conocer desde las primeras semanas de noviembre. Conversaciones *off the record* de políticos que transmitían a los diplomáticos norteamericanos sus preocupaciones en los ámbitos políticos, de seguridad nacional, de lucha contra la delincuencia, etcétera. La radiografía de los gobiernos fue expuesta con la amenaza de seguir ahondando más.

Así, en los primeros días de enero de 2011, un exbanquero hizo entrega al propio Assange de un nuevo caudal de datos relativos a información de diversas personas que evadían al fisco mediante cuentas establecidas en Suiza. La obtención de datos por parte de *Wikileaks* no ocurrió a través de un trabajo de un Hacker en los sistemas de información norteamericanos, sino que provino desde adentro de estos sistemas. Un joven militar entregó esta información para difundirla y exhibir la política exterior de su país.La obtención de esa información es referida por el diario *El Universal*:

> "El supuesto responsable de la mayor filtración de secretos en la historia de EU, el cabo Bradley Manning, sólo necesitó un disco CD etiquetado como música y un poco de pantomima para causar lo que puede ser una crisis diplomática sin precedentes."

[2] Cfr. *El País*, 10 de noviembre de 2010.

'Llegaba con un CD-RW (CD grabable) con música con la etiqueta de algo como 'Lady Gaga', borraba la música y grababa un archivo comprimido en partes', explicó el propio Manning al ex hacker que lo delató a las autoridades estadounidense, Adrian Lamo.

'Escuchaba y movía los labios a la canción 'Telephone' de Lady Gaga a la vez que sacaba posiblemente la mayor filtración de datos de la historia estadounidense', añadió Manning según los registros de los mensajes que mantuvo con Lamo a finales de mayo y obtenidos por la revista 'Wired', que los ha publicado.

'Servidores flojos, registros débiles, mala seguridad física, mala contrainteligencia, analistas de señales distraídos... la tormenta perfecta', terminó revelando el antiguo analista de inteligencia del Ejército estadounidense.

Entonces Manning, de 22 años, estaba destinado en la Base Operativa Avanzada Hammer, a unos 60 kilómetros al este de Bagdad (Irak).

Gracias a su puesto, Manning tenía acceso a dos ordenadores portátiles conectados a dos redes clasificadas del Gobierno estadounidense.

Una es SIPRNET (*Secret Internet Protocol Router Network*), una red utilizada por los Departamentos de Defensa y de Estado para sus comunicaciones confidenciales y por la que se transmiten los mensajes entre Washington y las embajadas estadounidenses en todo el globo que están siendo revelados por *Wikileaks*.

La segunda red a la que tenía acceso Manning era todavía más importante, *Joint Worldwide Intelligence Communications System*, porque es por la que circulan los documentos de clasificación 'TOP SECRET' o SCI ('Sensitive Compartmented Information' o información compartimentada sensible).

Durante meses, Manning tuvo acceso a los contenidos de estas dos estratégicas redes, básicamente dos internet de secretos.

'Si tuvieses acceso sin precedentes a redes clasificadas durante 14 horas al día, 7 días a la semana durante más de 8 meses, ¿qué harías? preguntó Manning a Lamo.

La respuesta vino poco después y Manning parece que se decantó por revelar lo que consideraba información que necesitaba estar 'en el dominio público'.

Manning fue arrestado a finales de mayo, poco después de contactar a Lamo y en junio fue acusado por las autoridades militares estadounidenses de incumplir el Código Militar.

Actualmente está encarcelado en la base de los Marines en Quantico, Virginia, a la espera de juicio en el que podría ser condenado hasta a 52 años de prisión, según señala la Red de Apoyo a Bradley Manning, un grupo que se ha formado para defender al ex analista militar.[3]

La obtención resulta claramente ilícita, pero ésta no ha sido utilizada para enderezar una acusación, pues sus fines han ido más allá de la denuncia pública y es por ello por

[3] Consultable en "Disco de música facilitó filtración en Wikileaks" en *El Universal*, martes 30 de noviembre de 2010.

lo que ha armado gran polémica. Hay quienes aprueban el que se haya dado a conocer lo que ya se sospechaba, pero de lo que no se tenía una prueba contundente. Por otro lado, hay quienes reprueban la obtención ilícita de esta información, pues consideran que celebrarlo motivaría a que distintos operadores de información hicieran lo propio.

El gobierno de Estados Unidos inició trámites para juzgar a Assange. Principalmente por el delito de espionaje, incluyendo con esto la aplicación de viejas leyes que datan de 1917. Para ello, y regresando al tema de este libro, el Departamento de Justicia, por conducto de un Tribunal en Virginia, solicitó a Twitter información sobre las comunicaciones de Assange con distintos colaboradores de Wikileaks. En el diario *El País* se publicó:

> "EE UU pide a Twitter información de las cuentas de colaboradores de Wikileaks. El Departamento de Justicia solicita datos de las cuentas de Julian Assange, una parlamentaria islandesa, el soldado encarcelado, un hacker y un programador.- Reclama, en un escrito con fecha 14 de diciembre y sellado en un tribunal de Virginia, los nombres de usuario, direcciones, registros de conexión, números de teléfono y transacciones (Óscar Gutiérrez - Madrid - 08/01/2011)"
>
> Enésimo asalto de la justicia estadounidense contra la web de filtraciones Wikileaks, su fundador, Julian Assange, y su entorno, mientras Washington aún se duele de la revelación el pasado 28 de noviembre de más de 250.000 cables diplomáticos enviados desde sus embajadas en todo el mundo al Departamento de Estado, con decenas de escándalos que han dejado al desnudo muchas claves de la política internacional estadounidense. En un intento de conocer cómo se ha gestado y ejecutado la fuga de información secreta, el Departamento de Justicia ha enviado una citación a la red social Twitter para que le facilite los datos personales de usuarios que tienen vinculación con la organización. Wikileaks ha informado a través de un comunicado que sospecha que ésta no es la única compañía a la que el Gobierno estadounidense ha reclamado información.
>
> La orden, cursada a través de un juzgado del Estado de Virginia, reclama a la empresa radicada en San Francisco que entregue los nombres de usuario, direcciones de correo, detalles de conexiones realizadas, números de teléfono, tiempos de conexión y pagos a través de Internet desde noviembre de 2009 hasta la actualidad.
>
> Desde esa fecha, Wikileaks ha liberado más de 700.000 documentos públicos con sello estadounidense. Entre ellos, el vídeo de la muerte en Bagdad de doce personas por fuego de Apaches norteamericanos y por cuya filtración está detenido el agente de inteligencia Bradley Manning. Este, según el soplo que le llevó a entrar en prisión, contactó con Wikileaks por primera vez precisamente en noviembre de 2009. De acuerdo con la orden judicial emitida el 14 de diciembre, la información requerida es "pertinente" y el material es importante "para una investigación criminal en curso", esto es, la causa de espionaje contra Assange que Washington intenta desarrollar desde el arresto de Manning.[4]

[4] **Los lazos de la diputada islandesa**
Entre el listado de personas cuyas cuentas están en el punto de mira se encuentran el propio Assange y una diputada islandesa, Birgitta Jónsdóttir, quien ha reaccionado con incredulidad al conocer la

Este caso de Wikileaks tiene su antecedente en uno similar, pero de menores proporciones ocurrido durante la guerra de Vietnam (finales de la década de los 60 y principios de la década de los 70 del siglo pasado). El caso fue el siguiente:

> "Hace treinta años en este mismo mes, el Presidente Nixon tomó su *New York Times* dominical del 13 de Junio de 1971 para ver la foto de la boda de su hija Tricia y él en el Rose Garden, liderando el costado izquierdo de la página principal. Junto a la foto, de lado derecho, estaba el título de la primera historia de Neil Sheehan sobre los documentos del Pentágono: 'Archivo de Vietnam: Estudio del Pentágono marca tres décadas de creciente participación de los Estados Unidos'.
>
> La noche del lunes, Junio 14, el Procurador General John Mitchell advirtió al *Times* vía telefónica y por telegrama contra futuras publicaciones, y el Martes 15 de Junio, el gobierno buscó y obtuvo una orden de restricción contra el *Times* – un mandato judicial posterior lo extendió al *Washington Post* cuando este periódico retomó la nota. La batalla legal que se produjo culminó el 30 de Junio de 1971 en una decisión 6-3 de la Suprema

petición recordando su condición de parlamentaria. Jónsdóttir, miembro del Parlamento islandés por el grupo El Movimiento, nacido al calor de la crisis económica que sufrió el país en 2008, simpatiza con el portal de Assange y le ha prestado su colaboración en varias ocasiones.

Prueba de la sintonía con el proyecto -al menos con el primer equipo que puso en marcha la web-, la parlamentaria logró que la Cámara de su país aprobara la Iniciativa Islandesa de Medios Modernos (IMMI), un proyecto de ley que pretende, al hilo de la filosofía de Wikileaks, blindar la ley de prensa más fuerte del mundo. Tras lograr el respaldo de los diputados, la IMMI se encuentra en el Parlamento para su adaptación a la legislación nacional.

Cuando Twitter recibió la petición de entregar esa información conoció también dos exigencias: la primera, que debía facilitar los datos en tres días, y la segunda, que no debía hacer público el requerimiento. Pese a ello, la red social ha informado a los afectados por la orden de que tienen 10 días para frenar el requerimiento vía legal. Si no lo hacen, según se desprende de la carta publicada en su blog por uno de los citados, Rop Gonggrijp, Twitter procederá a la solicitud de la justicia estadounidense. La red aconseja incluso en el escrito que utilicen consejo legal y recomienda las organizaciones Electronic Frontier Foundation y ACLU.

El soldado, el *hacker* y el programador

La justicia estadounidense también ha requerido amplia información confidencial del perfil en Twitter del soldado Manning; del *hacker* holandés Rop Gonggrijp y del programador estadounidense Jacob Appelbaum. Estos últimos, antiguos trabajadores de la organización dirigida por Assange. El fundador de Wikileaks se ha referido hoy a las intenciones de EE UU de recabar datos personales y secretos de Twitter: "Si el Gobierno iraní tratase de obtener esta información de los periodistas o activistas extranjeros, grupos de derechos humanos de todo el mundo se habrían manifestado", señaló Assange en un comunicado.

La red social de mensajes cortos (140 caracteres) se ha limitado a señalar que "para proteger los derechos de los usuarios es nuestra política notificar a los usuarios sobre el cumplimiento de la ley y de las solicitudes gubernamentales, para su información, a menos que se les impida por ley hacerlo". La compañía de San Francisco señala en su apartado dedicado a la privacidad de los contenidos que podría revelar la información de un usuario si "es razonablemente necesario para cumplir la ley, un reglamento o requerimiento legal; para proteger a una persona; para combatir el fraude, por motivos técnicos o de seguridad; o proteger los derechos o propiedades" de la red social. (Consultable en: http://www.elpais.com/articulo/internacional/EE/UU/pide/Twitter/informacion/cuentas/colaboradores/Wikileaks/elpepuint/20110108elpepuint_10/Tes?print=1)

Corte de los Estados Unidos para quitar las restricciones – pudiendo ser el caso de la Suprema Corte más importante sobre libertad de prensa.[…]

Los informes secretos y la evidencia secreta:

En los siguientes días, este Libro electrónico informativo añadirá copias de documentos específicos en los Papeles del Pentágono que fueron citados por el gobierno en varios documentos legales públicos y secretos que crean un daño inmediato a la seguridad nacional de Estados Unidos. El investigador principal del Archivo, John Prados, llevó a cabo un exhaustivo proyecto de referencia cruzada usando los informes secretos recientemente desclasificados, llevados por el gobierno a las cortes, junto con cada una de las ediciones de los periódicos, incluyendo la versión rústica del *New York Times* (altamente condensada y selectiva), el multivolumen de la versión de la Imprenta del Gobierno (oficialmente desclasificada), la edición leída del Senador Mike Gravel en la grabación del subcomité del Senado y publicado posteriormente por Beacon, y cuatro volúmenes de negociaciones (que Daniel Ellsberg no filtró) desclasificados en 1977.[5]"

En Estados Unidos se respetó la libertad de prensa sobre la información filtrada en aquel entonces. ¿Será por eso que *Wikileaks* utilizó a los diarios? Lo cierto es que, independientemente del caso Assange, *Wikileaks* también permitió conocer un aspecto de la red contra el que los gobiernos no están preparados: el verdadero fenómeno

[5] But out of the gobbledygook, comes a very clear thing: [unclear] you can't trust the government; you can't believe what they say; and you can't rely on their judgment; and the – the implicit infallibility of presidents, which has been an accepted thing in America, is badly hurt by this, because it shows that people do things the President wants to do even though it's wrong, and the President can be wrong." -- H.R. Haldeman to President Nixon, Monday, 14 June 1971, 3:09 p.m. meeting.
Thirty years ago this month, President Nixon picked up his Sunday New York Times on June 13, 1971 to see the wedding picture of his daughter Tricia and himself in the Rose Garden, leading the left-hand side of the front page. Next to that picture, on the right, was the headline over Neil Sheehan's first story on the Pentagon Papers, "Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U.S. Involvement."
On Monday evening, June 14, Attorney General John Mitchell warned the Times via phone and telegram against further publication; and on Tuesday June 15, the government sought and won an restraining order against the Times – an injunction subsequently extended to the Washington Post when that paper picked up the cause. The epic legal battle that ensued culminated on June 30, 1971 in the U.S. Supreme Court's 6-3 decision to lift the prior restraints – arguably the most important Supreme Court case ever on freedom of the press. […]
The Secret Briefs and the Secret Evidence:
In coming days, this Electronic Briefing Book will add copies of the specific documents in the Pentagon Papers that were cited by the government in various public and secret legal papers as creating immediate harm to U.S. national security. Archive senior fellow John Prados has carried out an exhaustive cross-referencing project using the recently-declassified secret briefs submitted by the government to the courts, together with each of the various editions of the Papers, including the New York Times paperback version (highly condensed and selective), the multivolume Government Printing Office version (officially declassified), Senator Mike Gravel's edition read into a Senate subcommittee record and subsequently published by Beacon, and the four negotiating volumes (which Daniel Ellsberg did not leak) declassified in 1977. (Traducción de Ulises Quero García).

de la red. ¿En qué consiste? En que lo primero que intentó el gobierno norteamericano fue cancelar la página web de *Wikileaks*, que el *DNS Wikileaks* dejara de funcionar. Pero no sirvió. *Wikileaks* encontró alojo en otros portales. Entonces comenzaron los ataques para denegar el servicio. Un método utilizado con frecuencia por los *hackers*. Esto permitió observar de qué manera los gobiernos, de manera institucional, atacan páginas en internet, cuya frecuencia y número hacen que la página electrónica no pueda resistir.

Esta clase de ataques también develaron que China lo ha hecho contra páginas de enemigos comerciales (caso Google) y Estados Unidos contra Irán, que está obstinada por tener armas nucleares. El ataque indiscriminado vulnera los sistemas de cómputo y los puede inutilizar. Del mismo modo, los *hackers* adherentes a la causa de *Wikileaks* hicieron algo inédito: la reproducción en distintos portales del mundo de la información de *Wikileaks*, algo que no podía contrarrestar Estados Unidos.

Asimismo, estos mismos hackers atacaron las páginas que en su momento habían negado el alojo a *Wikileaks*. El fenómeno de la red destacó que no hay una solución concreta a un problema global. En la red (y en estas nuevas redes sociales) está el secreto para resolver problemas de esta dimensión. Todo esto ha motivado la iniciativa para que los usuarios de internet tengan una identificación (única) para acceder al servicio. Recientemente (2021), El Reino Unido de la Gran Bretaña autorizó la extradición de Julian Assange a Estados Unidos de América por el delito de espionaje y el titular del Ejecutivo en México tomó una postura interesante sobre la defensa de Assange.

IV. EL CASO SNOWDEN

Edward Snowden fue un empleado de las instituciones especializadas en seguridad e inteligencia de los Estados Unidos de América. Su caso fue la secuela de otro similar conocido como *Wikileaks*, mediante el cual se dio a conocer al público diversos documentos confidenciales que exponían el trabajo que se realizaba desde la diplomacia para hacerse de información privilegiada.

Aquel primer escándalo le costó la persecución y el asilo político forzado a Julian Assange. Pero, a diferencia de aquél, Snowden era norteamericano y sabía, por haber estado dentro del gobierno hasta dónde llegaba su intrusión en las comunicaciones privadas.Sin embargo, y con la amenaza de ser acusado de delitos muy graves y de ser perseguido con más ferocidad por el Estado vigilante, Snowden aportó los elementos para exhibir al gobierno de los Estados Unidos y sus prácticas de vigilancia hacia sus propios ciudadanos en franca violación a sus libertades.

Como es de suponer, Snowden quedó atrapado en ese limbo en el que la ética lo contrapone con las leyes de su país y, a pesar de sus fines, tuvo que huir hacia un estado protector, tradicionalmente antagónico como es Rusia. El caso de Snowden da cuenta que la lucha contra los ataques en la red (cibereterrorismo, ciberguerra),

paulatiamente se ha convertido en el pretexto para enfilar sus baterías hacia el uso doméstico, invadiendo los aspectos más íntimos de los ciudadanos, lo que no solo resulta ilegal, sino que alimenta el control sobre la población al punto de influir de manera definitiva en el curso de la economía y la vida de los usuarios de los dispositivos. Con esta invasión queda al descubierto que la intimidad es un bien jurídico valioso en extinción.

V. LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN, LA COMUNICACIÓN Y EL DERECHO PENAL

La historia se relaciona con el derecho penal por los bienes jurídicos en conflicto, al revelar la violación institucional de la intimidad de todos los usuarios de las comunicaciones y lo que implica realizar actos como la revelación de secretos que importan la seguridad del Estado. Así también hay una relación con la responsabilidad de los aparatos organizados de poder que, de manera institucionalizada y bajo la simulación de actos jurídicos invaden la privacidad de todos los gobernados.

Así, quedan de manifiesto el uso que se le da a la *Ley de Vigilancia de la Inteligencia Extranjera de 1978* (EEUU) y al Tribunal secreto, *El Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos de América,* que se instituyó con el fin de legalizar las intervenciones de comunicaciones.

Y a pesar de que, a consecuencia del caso Snowden ya no existe tal intrusión, el caso *silk road*, deja en claro que tal vez ya hubo una respuesta gubernamental que no ha sido debidamente acatada. Las tecnologías han avanzado demasiado como para dejar de ser utilizadas, por ejemplo los detectores de retina, las cámaras que se prenden de manera remota, los vehículos de conducción totalmente automática, etcétera.

En el documental realizado por Oliver Stone sobre este punto, aparece un personaje en particular, el jefe de Snowden, justifica la actuación, le pone en claro que también él está bajo vigilancia y le deja una consigna que debe utilizar durante su actuación como espía: "El nuevo campo de batalla está en todas partes. No estarán en una trinchera o cubriéndose de un mortero". La tercera guerra mundial habrá de librarse de manera inevitable en el ámbito virtual, impidiendo las comunicaciones y el uso de las nuevas tecnologías.

VI. EL CASO MEXICANO

La ciberseguridad consiste en el cuidado que tiene un Estado para resguardar la información y las comunicaciones.[6] El hackeo a que hemos hecho referencia en las

[6] **La ciberseguridad como bien jurídico protegido** "Las característica del Ciberespacio, hace que la seguridad cibernética juegue un papel central en su aplicación en el contexto de un Estado de Derecho,

primeras líneas fue confirmado por el titular del Ejecutivo mexicano en conferencia de prensa de 30 de septiembre de 2022. Ratificó que era real su mal estado de salud, las atenciones que recibió derivado de sus distintas enfermedades, pero, sobre todo, manifestó que la filtración de información es real.

En México, la legislación prevé la sanción para aquellas personas que revelan secretos, como también existe el derecho a la libertad de prensa. En lo que hace a los aspectos específicos, el gobierno deberá iniciar las denuncias correspondientes para investigar quién realizó el supuesto hackeo (que bien podría haber sido un robo de información a través de medios físicos y no a distancia). El Código Penal Federal prevé lo siguiente:

> **Artículo 211 bis 2**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
>
> **Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.**

---

así como en el juego de relaciones internacionales, llegando a ser una constante, presente, de una u otra forma, en todos los intereses en juego del nuevo ámbito relacional cibernético. Esta omnipresencia de las relaciones cibernéticas, en todos sus aspectos, técnicos, sociológicos, jurídicos, económicos y políticos, hace emerger al Ciberespacio –y las relaciones electrónicas que lo sustentan- como un nuevo valor, un nuevo bien jurídico digno de protección –barrera de protección jurídica anticipada- , de carácter universal, que deberá servir para configurar nuevos tipos penales, con independencia de los ya existentes y, entre los que destaca por su importancia para hacer viable el bien principal, la seguridad cibernética y el derecho al uso seguro de Internet. La seguridad cibernética como garante de un estándar de seguridad colectiva en el ámbito relacional constituido por el Ciberespacio, es un área de confluencia de intereses de la más variada índole (públicos y privados, estatales, comerciales, industriales, individuales, sociales, militares, de inteligencia o policiales). La seguridad cibernética es un bien jurídico que adquiere una dimensión institucional y supraindividual, cuyo objeto jurídico de protección inmediato es la seguridad colectiva, lo que no impide que determinados bienes jurídicos individuales constituyan un objeto inmediato de protección, en una situación valorativa en relación al bien supraindividual. Los bienes jurídicos son unidades funcionales relativas, referidos al orden social del momento, y sus objetivos. La seguridad cibernética es una entidad nueva de protección, referida a los procesos y funciones que ha de cumplir el sistema, para que estén aseguradas las bases y condiciones, esencialmente los bienes jurídicos individuales. Frente a los medios de comisión cibernéticos, de gran potencia lesiva, la seguridad cibernética tiene entidad suficiente para recibir un tratamiento autónomo como bien jurídico penalmente relevante. Como bien jurídico, junto a los intereses individuales protegidos, se puede percibir algo que transciende y que se podría definir como 'el derecho que todos tienen para el desenvolvimiento normal de sus vidas en paz, sosiego, bienestar y tranquilidad' (STS de 9 de octubre de 1984) en el ámbito del Ciberespacio. Por todo ello, tal vez sería conveniente establecer en el Código Penal, un tipo específico, relativo a los delitos contra la seguridad cibernéticas, en el Título relativo a los delitos contra la seguridad colectiva, que conviviría con subtipos referidos a bienes jurídicos individualizados como la libertad de expresión, la privacidad, la intimidad, el secreto de las comunicaciones, la seguridad del Estado, la prevención y persecución del delito, o los datos de carácter personal, u otros." José María Molina Mateos http://www.abogacia.es/2014/09/15/la-ciberseguridad-como-bien-juridico-protegido/ consultado 15 de sep. de 2014 17:41

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

De lo anterior, como siempre, nos salta la duda si habrá estado protegida esa información de manera adecuada por un mecanismo de seguridad. [7] Para atender a

[7] Jesús Antonio Molina Salgado escribe una crítica sobre esta legislación:
"La legislación mexicana en materia de delitos informáticos dista mucho de ser perfecta, es sólo el primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país. Algunos de los defectos del Código Penal Federal en esta área son los siguientes:
a) Contempla que constituye el delito sólo si se accede un sistema informático protegido por un mecanismo de seguridad. Esto es tan absurdo como si dijéramos que para que se diera el delito de allanamiento de morada es necesario que la casa habitada cuente con un candado, llave, portón o cadena protectora. La justicia no puede reducirse sólo a aquellos quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad. ¿O qué acaso el que tu computadora esté conectada al Internet significa que cualquiera puede justificadamente, borrar o destruir archivos, sólo porque no está protegida por algún mecanismo de seguridad?

estas cuestiones, en el proyecto de código penal nacional se propuso una solución a través de la interpretación auténtica del legislador, de acuerdo con la norma internacional ISO 27000, sobre lo que debe entenderse por mecanismo de seguridad que tantos dolores de cabeza causa en la práctica.[8]

Los delitos señalados por supuesto no alcanzan para atacar el libre trabajo de la prensa, solo a quien obtuvo esa información de manera ilícita y la transmitió. Estamos conociendo apenas en la punta del iceberg. En los próximos días y meses podremos observar el impacto de la información obtenida y difundida por los medios impresos y digitales.

¿Será esta la oportunidad para que el Estado mexicano atienda puntualmente los vacíos en torno a la ciberseguridad? ¿Lo motivará a firmar y ratificar el Convenio de Budapest (contra la cibercriminalidad)? ¿Lo motivará a revisar la legislación en torno la legislación penal única, así como a la ciberseguridad y los delitos informáticos? ¿Será otra ocasión perdida?

b) El Código Penal no define qué debe entenderse por 'mecanismo de seguridad'. ¿Qué es un mecanismo de seguridad de un sistema informático?, ¿Un *password*? ¿Un candado contra robo (físico)?, ¿Un *firewall*?, ¿Un sistema criptográfico de llave pública?, o simplemente ¿Tener la computadora encerrada en un cuarto bajo llave o con un guardia de seguridad a un lado?. Esta vaga redacción sin duda traerá innumerables problemas de interpretación a la hora de que le toque a un juez analizar un caso concreto.

c) Nuestro código no contempla todos los tipos más comunes de ataques informáticos. El Capítulo II adicionado en virtud de la reforma del 17 de mayo de 1999, de entrada está titulado de manera incorrecta: 'Acceso Ilícito a Sistemas y Equipos de Informática'. Aunque su articulado (Arts. 211 bis 1 al 7) no habla en todo momento de acceso ilícito, el título del capítulo sí enfoca su contenido a accesos ilícitos precisamente.

El problema radica en que muchos ataques informáticos se perpetran sin necesidad alguna de acceder directamente un sistema informático. El mejor ejemplo es el ataque de 'Denegación de Servicios' (*Denial of Services o Distributed Denial of Services*), cuyo objetivo no es 'modificar, destruir o provocar pérdida de información', como reiteradamente lo establece el Código Penal Federal, sino simplemente imposibilitar o inhabilitar un servidor temporalmente para que sus páginas o contenidos no puedan ser vistos por los cibernautas mientras el servidor está caído" Molina Salgado, Jesús Antonio, *Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial,* (col. Breviarios Jurídicos), Porrúa, México, 2003, pp. 69 –70.

[8] Acceso ilícito a sistemas y equipos de informática

[…] "**Por mecanismo de seguridad se entenderá toda herramienta o técnica física o lógica, material o virtual, que sirva para preservar la confidencialidad, la integridad, y la disponibilidad de la información, para impedir el acceso libre a datos o información contenida o para salvaguardar algún bien informático.**

Por base de datos se entenderá el conjunto ordenado de información almacenado en cualquier medio informáticos, así como los relativos a una persona identificada o identificable."