INTERNET COMO INSTRUMENTO DE VIGILANCIA: CASO SNOWDEN A HOY

Spratt, Francisco[1]

Grupo de investigación de Ciberespacio

Palabras clave: ciberespacio, vigilancia, privacidad, información

Cita sugerida: Spratt, F. (2023). Internet como instrumento de vigilancia: Caso Snowden a hoy. *Centro de Estudios Estratégicos de Relaciones Internacionales.*

[1]Spratt, F. (13 de julio de 2023). Licenciado en Relaciones Internacionales en la Universidad del Salvador. Contacto: franciscospratt@gmail.com

1. Las revelaciones de Snowden

El 9 de junio del año 2013, un joven estadounidense llamado Edward Snowden aclama ser la fuente por la que, un par de días antes, el diario británico The Guardian hacía mención de una serie de documentos confidenciales en los que denunciaba un plan de vigilancia sistemática por parte del gobierno de los Estados Unidos, principalmente a partir de los programas PRISM y X-KeyScore.

Con el transcurso de las semanas, en un proceso dinámico, se publicaron una serie de documentos confidenciales mostrando las técnicas de recolección de información y abuso a la privacidad que estaba empleando el gobierno de los Estados Unidos, principalmente a partir de la National Security Agency (NSA por sus siglas en inglés), lo que generó un repudio en la comunidad internacional, pérdida de confianza local e internacional de los Estados Unidos y una serie de reformas en el ciberespacio, comenzando por la Unión Europea. En este artículo propongo analizar el mismo campo y prácticas de ciberpoder por parte del gobierno de los Estados Unidos a partir de algunas de sus instituciones, denotando que 10 años más tarde, la realidad no es muy distinta.

Luego del atentado del 11 de septiembre a las Torres Gemelas, y con la necesidad de una rápida acción política, se aprueba con una amplísima mayoría tanto de la Cámara de Representantes como de la Cámara de Senadores, la “Ley Patriota”. En palabras de Quintanar (2016), surge con el objetivo de “subordinar los derechos ciudadanos a la vigilancia con objeto de incrementar la seguridad del Estado” (Quintanar, 2016, p.163). Esta Ley “suspendió” en gran medida el derecho a la privacidad tanto de ciudadanos estadounidenses pero sobre todo extranjeros (Espino, 2007), y se amplió el concepto de terrorista para la libre vigilancia cibernética desde “causa probable” a causa “pertinente” para la libre obtención de historiales médicos, transacciones bancarias, llamadas telefónicas, etc. (Greenwald, 2014, p.164).

Con la elocuente exposición de documentos confidenciales por parte de los Diarios Washington Post y The Guardian, a los cuales Snowden había contactado a través de los periodistas Edward Greenwald y Laura Poitras, para que los publicaran de la manera que creyeran más óptima, la comunidad internacional hizo alusión a las prácticas de vigilancia y recolección de información y comenzaron a denunciarlo y buscar respuestas: Mandatarios estatales se vieron expuestos como víctimas de este espionaje, caso Dilma Rousseff, Angela

Merkel y François Hollande, entre otros, los cuales exigieron respuestas en organismos internacionales como la ONU; organismos no gubernamentales como Human Rights se abocaron más al asunto denunciando en el transcurrir de los siguientes años; y algunos usuarios de las distintas empresas de internet, como lo fue en Facebook, buscaron llevarlo a instancias judiciales.

2. Necesidad de reformas

Bajo las diversas denuncias tanto en el ámbito internacional como en el nacional, en el Poder Legislativo de los Estados Unidos y su Congreso se presenta en 2015 la "Ley de Libertad Estadounidense" (Freedom Act en inglés), la cual luego se promulga, buscando prohibir la recolección masiva de datos, proveer más transparencia, privacidad y más libertad a los ciudadanos, "expandiendo las capacidad del Congreso" para vigilar las acciones de organismos como la NSA en la recolección de información y vigilancia (United States 114th Congress, 2015).

Dicha Ley, en términos generales, es una reforma de la tan cuestionada "Ley Patriota" por las denuncias a partir de las revelaciones de documentos confidenciales facilitados por Edward Snowden. La misma contemplaba modificaciones significativas para las prácticas de los Organismos de Inteligencia de los Estados Unidos que emplearon para recolectar masivamente metadata (Mora, p.38).

Como se explicó anteriormente, el resto de la comunidad internacional no estuvo exenta de las prácticas de vigilancia por parte de la NSA, por la que muchos Estados han invertido y generado distintas políticas entorno a la ciberseguridad nacional, donde aquí destaco tres casos:

Aunque pueda sorprender, en primera instancia podemos ejemplificar con Estonia, siendo un caso valedero en políticas de ciberseguridad, promoviendo la cooperación en ciberseguridad con aliados y socios tecnológicos, legislativos y diplomáticos, leyes para la protección nacional de su ciberseguridad, y la intención de aplicar el derecho internacional a los conflictos y la guerra cibernética (Bravo, 2022).

En segundo lugar, en el Reino Unido existen leyes como la "Ley de Protección de Datos", donde se establecen sanciones relevantes tanto por el incumplimiento de las mismas por supuesto, como para los directivos con actos de negligencia y la falta de medidas de

seguridad adecuadas para proteger los datos personales de los usuarios. Sumado a ello, poseen la Institución "Centro Nacional de Seguridad Cibernética (NCSC por sus siglas en inglés), la cual desarrolla habilidades digitales para las las distintas empresas cibernéticas del Reino Unido a fin de disuadir, mitigar riesgos y efectos de los ataques, y desarrollar una evolución constante en la defensa cibernética.

En tercer lugar, cabe nombrar a la Unión Europea, quien concentró gran parte de sus actividades en torno a la ciberseguridad luego de las revelaciones de Edward Snowden, en su Programa denominado "Horizonte 2020" para los años 2014 al 2020, lo cual finalizado el programa, siguieron el lineamiento con el subsiguiente programa "Horizonte Europa" (en vistas al 2021-2027). Ambos programas refieren a la fuerte competitividad tecnológica y científica dentro de la región, invirtiendo en la Ciencia, la Tecnología y desafíos globales entre ellos el de la ciberseguridad.

3. Denuncias post Snowden

Si bien se generaron varias reformas en el cuidado del ciberespacio y la protección de los datos de los ciudadanos y Estados, el periodo comprendido desde el 2013 ha habido múltiples denuncias con más y menos evidencia expuesta como es el caso de Francés Haugen, ex empleada de Facebook, quien expuso documentos de la empresa y denunció el accionar de la misma en la recolección de información en post de debilitar la democracia.

Otro caso es el de Cambridge Analítica (empresa británica de consultoría analítica), la cual fue denunciada en 2018 por utilizar información adquirida a Facebook. Catalogada como la denuncia más grave y sustentada en contra de Facebook, se acusa de haber utilizado información personal para influir en las elecciones presidenciales de los Estados Unidos en 2016.

El año pasado, en febrero del 2022, los senadores Ron Wyden y Martin Henrich por el partido demócrata y miembros del Comité de Inteligencia del Senado, volvieron a denunciar a la Agencia Central de Inteligencia (CIA) por la recopilación masiva de información, así como los problemas de esta institución en el manejo de información de los estadounidenses.

Sumado a ello, si bien se publicaron programas en plan de vigilancia y recolección de información atentando contra la seguridad, hoy en día funcionan 5 nuevos programas de la NSA para recolectar información y vigilar (con distintos nombres y similares funciones

previo al “fenómeno Snowden”) que Organismos de Derechos Humanos han publicado. Esto muestra la aún vigente necesidad de mejorar la inteligencia en el ciberespacio para la protección de la información. (American Civil Liberties Union, Center For Democracy & Technology, 2015).

4. Reflexión final

A pesar de notar que son numerosas las mejoras tecnológicas y de inversión en el campo de la ciberseguridad, remarcando solo algunos ejemplos sobresalientes dentro de la comunidad internacional, podemos concluir que la recolección de información y la vigilancia del aparato cibernético estadounidense es un asunto aún latente para ocuparse y remarcar, en el cual no parecen haber aún medidas concretas que resuelvan esta problemática, denunciada y hasta evidenciada en varias oportunidades.

El ciberespacio es un ámbito complejo, desafiante en su estudio y en el que la modernización de la tecnología requiere de una fuerte y constante resiliencia cibernética para proteger la privacidad de todos los ciudadanos y la ciberseguridad estatal. Si bien se está invirtiendo cada vez más en el campo del ciberespacio para protegerla, aún no se han resuelto las mismas problemáticas que Edward Snowden comenzaba a denunciar hace 10 años.

Bibliografía

- American Civil Liberties Union; Center For Democracy & Technology. (Mayo, 2015): *"Secret Surveillance: Five Large-Scale Global Programs"*. Recuperado de: https://cdt.org/wp-content/uploads/2014/09/cdt-aclu-upr-9152014.pdf

- Bravo Jorge, (2022): "Qué aprender de los países líderes en ciberseguridad". Recuperado de: https://dplnews.com/que-aprender-de-los-paises-lideres-en-ciberseguridad/

- Global Voices, Kudzai Chimhangwa. (2022): *"Usar la ley como arma: Nueva frontera de Zimbabue para reprimir derechos digitales"*. Recuperado de: https://es.globalvoices.org/2022/05/11/usar-la-ley-como-arma-nueva-frontera-de-zimbabue-para-reprimir-derechos-digitales/

- Human Rights Watch (2017): *"EE.UU: Nueva información sugiere que se vigila a los ciudadanos"*. Recuperado de: https://www.hrw.org/es/news/2017/10/25/ee-uu-nueva-informacion-sugiere-que-se-vigila-ciudadanos

- Mora Piñeros, Sahian Manuela. (2023): *"Protección Internacional de la Privacidad y Regulación del Uso de Datos Personales, ¿una Utopía?: Análisis del Caso de Estados Unidos en la Era Posterior a las Revelaciones de Edward Snowden"*. Recuperado de: https://repository.javeriana.edu.co/bitstream/handle/10554/63244/Trabajo%20de%20grado-%20Manuela%20Mora%20.pdf?sequence=1&isAllowed=y

- Diario "Vice" (2020): *"How the U.S. Military buys location data from ordinary apps."*. Recuperado de: https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

- Diario "Vice" (2022): *"Revealed: US Military bought mass monitoring tool that includes Internet Browsing, Email Data"*. Recuperado de: https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data

- Wydenn Ron (10 de Febrero 2023): *"Wyden and Heinrich: ´Newly declassified documents reveal previously secret CIA Bulk Collection, problems with CIA handling of American´s information"*. Recuperado de: https://www.wyden.senate.gov/news/press-releases/wyden-and-heinrich-newly-declassified-documents-reveal-previously-secret-cia-bulk-collection-problems-with-cia-handling-of-americans-information