La preocupante relación entre el espionaje digital y las campañas electorales en América Latina

Por: María Agustina Puebla[1]

Para citar: María Agustina Puebla, "La preocupante relación entre el espionaje digital y las campañas electorales en América Latina" en Blog Revista Derecho del Estado, 14 de agosto de 2023. Disponible en: https://blogrevistaderechoestado.uexternado.edu.co/2023/08/14/la-preocupante-relacion-entre-el-espionaje-digital-y-las-campanas-electorales-en-america-latina/

Introducción

La llegada del siglo XXI trajo consigo avances tecnológicos inimaginables en otras épocas. El internet ha crecido a pasos agigantados. De la misma manera, el software de las computadoras, celulares y tablets es cada vez más sofisticado. Atrás quedaron los tiempos de los grabadores de voz, las cámaras fotográficas analógicas, las videograbadoras, los manuscritos (en sentido literal) y la correspondencia tradicional. Incluso, existe la tendencia a digitalizar los expedientes judiciales y administrativos en países de la región, como Argentina, por ejemplo.

Sin embargo, se podría decir que el uso de la tecnología también es dañino cuando no se utiliza con un fin noble. En un mundo utópico, la tecnología mejora la calidad de vida de las personas, permite facilitar las comunicaciones entre pares, agilizar las tareas escolares y laborales y ser un medio de entretenimiento en los tiempos libres. A pesar de ello, vivimos en el mundo del ser (y no en el del deber ser), por lo tanto nos encontramos con un uso 'non sancto' de los medios informáticos. Los delincuentes ("tradicionales" y de cuello blanco) se nutren de programas de espionaje para, efectivamente, llevar adelante su accionar antijurídico. De esta manera, se vulnera el derecho a la intimidad y a la inviolabilidad de las comunicaciones y correspondencia. Pero la situación es aún más peligrosa cuando son los propios gobiernos quienes se colocan en este rol delictivo, ya que vulneran los derechos humanos de los ciudadanos, que en principio deberían defender

Breve definición de delitos informáticos. El espionaje digital (o informático)

Una primera aproximación al concepto de delitos informáticos puede ser definida como a *"(…) las conductas que afectan el software o soporte lógico de un sistema informático (…)"* (Jijena, 1994 y Moscoso, 2014 en Mayer Luz y Vera Vega, 2020, p. 3) Sin embargo, catedráticos como Davara Rodríguez y Telles Valdés consideran que no es adecuado hablar de "delitos informáticos" como tales, ya que no existe

ni se atiende a la necesidad de una tipificación en la legislación penal para que pueda existir un delito. (Acurio Del Pino, s/f, pág. 9)

A su vez, este universo de delitos está compuesto por tres figuras: sabotaje, espionaje y fraude informático. A su vez, si estos delitos son perpetrados a través del uso de internet, se afecta a un determinado bien jurídico, denominado "funcionalidad informática". Este puede ser definido como un "(… *conjunto de condiciones que posibilitan que los sistemas informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo.*" (Mayer, 2017 en Mayer Lux y Vera Vega, 2020, p. 4)

Mayer Lux y Vera Vega (2020) afirman que los delitos informáticos en general, y particularmente el delito de espionaje digital (o informático), acarrean dificultades de interpretación y delimitación. Desde la dogmática penal, el análisis de la figura es todavía incipiente, por un lado; y por el otro, el espionaje informático tiene poco tratamiento doctrinario.

Los autores mencionados ut supra sostienen a su vez que este espionaje abarca diversas conductas en su forma de ejecución y gravedad. Por ejemplo, comprende acceso indebido a sistemas informáticos (con el subsiguiente conocimiento de la información almacenada en el dispositivo) hasta el acceso y obtención indebida de datos o programas. Mayer Lux y Vera Vega (2020) también afirman que existen tres variables interrelacionadas en este tipo de delitos: la forma de ejecución, la gravedad y el hecho de que la conducta se lleve a cabo en el ciberespacio. A su vez, "(…) puede impactar negativamente en diversos bienes jurídicos, ya sea individuales o colectivos (por ejemplo, la intimidad o seguridad nacional), lo que a su vez depende de la clase de información con la cual se vincule" (Mayer Lux y Vera Vega, 2020, p. 30)

Casos de espionaje digital en América Latina

De acuerdo con Fionnuala Ni Aoláin, experta de la ONU, varios países y empresas privadas utilizan la "retórica de la lucha contra el terrorismo y la seguridad" para justificar un importante aumento del despliegue y uso de tecnología de vigilancia de vanguardia. No existe regulación alguna, lo que acarrea un "devastador" coste para los derechos humanos.

A su vez, durante la última sesión del Consejo de Derechos Humanos la relatora especial de la ONU sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, advirtió de un alarmante aumento en el uso de "tecnologías intrusivas y de alto riesgo". Entre ellas se encuentran los drones, la biometría, la inteligencia artificial (IA) y los programas espía, que se están intensificando en nombre de la lucha contra el terrorismo, sin tener debidamente en cuenta el Estado de derecho, la gobernanza y los derechos humanos. (Noticias ONU, Marzo 2023).

Por otro lado, el comunicado de prensa emitido en septiembre del año 2022 por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos humanos advierte sobre los instrumentos de espionaje y vigilancia. Nuevamente la ONU reafirma que los considera una amenaza a la intimidad y a los derechos

humanos. En el mismo, se explica que los gobiernos abusan de las herramientas de injerencia (también conocido como “spyware”). Además, recomienda a los Estados tomar todas las medidas necesarias para evitar la proliferación de estos instrumentos. Por último, considera que “(…) la intrusión de las autoridades en los aparatos electrónicos solo debería usarse como recurso de última instancia “para evitar o investigar actos específicos que representen amenazas graves a la seguridad nacional o delitos de gran entidad (…)” (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2022).

En América Latina, el espionaje a campañas electorales mediante el uso de Internet se ha detectado en varios países en los últimos años, por lo tanto, constituye un fenómeno digno de estudio. Algunos autores le dan un nombre particular a esta problemática. Por ejemplo Cárdenas López (2018) lo ha denominado “Watergate criollo”. De esta manera se refiere a la “(…) compleja técnica de interconexión tecnológica, que involucra a empresas occidentales globalizadas y afecta seriamente la democracia y se extiende sin que autoridades locales y judiciales puedan controlar la avanzada.” (Cárdenas López, 2018)

A su vez, informa que en la región se han detectado aproximadamente 11 países vinculados a campañas de phishing, malware, espionaje y sitios o cuentas falsas. De hecho, la ONG Derechos Digitales ha publicado informes sobre el uso ilegal del software espía en la región. Allí se detalla que países como Brasil, Chile, Colombia, Ecuador y México (entre otros) utilizaron el sistema Galileo o DaVinci.

De acuerdo con Cárdenas López (2018), estas denominaciones son nombres comerciales para Remote Control System (RCS). Por otro lado, Argentina, Guatemala, Venezuela, Perú y Paraguay sólo iniciaron negociaciones, pero no se brinda información sobre posibles ventas consumadas. El autor mencionado ut supra también menciona el caso de la empresa Haking Team, la cual “(…) argumentó en su defensa que vendían herramientas de hackeo a las agencias de gobierno para detectar a criminales, incluidos terroristas, pedófilos y traficantes de droga y que cancelan sus contratos si sus clientes utilizan sus programas para romper la ley.” (Cárdenas López, 2018).

Es necesario destacar el caso de las elecciones presidenciales de Panamá en el año 2014. A través de una filtración realizada por Wikileaks, se demostró que el gobierno del presidente Martinelli pagó durante tres años 750 mil dólares para realizar espionaje en las telecomunicaciones desde el gobierno local. Sin embargo, los argumentos esgrimidos por el gobierno eran completamente distintos: supuestamente era utilizado para descubrir autores de delitos como extorsión y secuestros. A pesar de esta excusa, la filtración de documentos anteriormente mencionada demuestra que las negociaciones entre la empresa Remote Control System y el gobierno panameño incluyen explícitamente la palabra “elecciones.”

También se puede mencionar el espionaje a jueces y al árbitro electoral en Ecuador, en el año 2014. El grupo Haking Team entra en escena nuevamente: esta vez sus programas fueron utilizados por la SENAIN (Secretaria Nacional de Inteligencia) para espiar a jueces, miembros del Consejo Nacional Electoral y

partidos políticos opositores, de acuerdo con lo explicado por Cárdenas López (2018).

Por último, otro caso que debe llamar la atención de organismos internacionales y de los gobiernos de la región es el espionaje que llevó adelante Estados Unidos en América Latina en el siglo XXI. La Escuela de las Américas en Panamá es una institución que (al parecer) quedó enterrada en el siglo pasado, junto con el Plan Cóndor y otras atrocidades que se produjeron en el continente con el aval de los Estados Unidos. Sin embargo, el diario O'Globo publicó en el año 2013 que los países de la región habían sido espiados, luego de filtraciones de ex trabajadores de la Agencia de Seguridad Nacional. En este caso, el programa informático utilizado fue Prism, que sirvió para intervenir de manera masiva las comunicaciones en Internet (Cárdenas López, 2018). Las víctimas de este espionaje ilegal fueron Dilma Roussef en Brasil y el candidato Peña Nieto en México. Este último sufrió interferencias en su teléfono celular y en sus redes sociales.

Conclusión

A lo largo de este artículo se ha podido revisar el concepto de delito informático. Si bien es un concepto propio de la dogmática penal, es fundamental conocer de qué se está hablando a la hora de analizar los casos de espionaje en América Latina. Será tarea de los juristas desarrollar aún más el concepto, los alcances, los elementos del tipo y la antijuridicidad de los delitos informáticos. Estamos, sin dudas, frente a un nuevo universo de delitos, en constante expansión. Sin embargo, es necesario reconocer que los penalistas están frente a una ardua tarea, ya que la vorágine del universo digital hace que en dos años, probablemente, estemos hablando de otras herramientas de espionaje ilegal; y las actuales queden obsoletas.

De la misma manera, es necesario reflexionar acerca del comportamiento de los gobiernos que recurren a estas herramientas para espiar a sus opositores en campañas políticas. Como se dijo anteriormente, se vulnera el derecho a la intimidad y a la inviolabilidad de la correspondencia de los candidatos (o de otros funcionarios públicos en ejercicio).

A pesar de ello, también se vulneran los mecanismos constitucionales para garantizar una democracia sana en los diversos países de la región. ¿Qué hace el gobierno, como institución, con la información que se recauda? ¿La utiliza para amedrentar a los opositores? ¿Para conocer cuáles son sus candidaturas, y de esta manera sabotear las mismas? ¿Para difundir información falsa sobre los candidatos u opositores al gobierno de turno? ¿Para ejercer más poder en la región, al estilo de un neocolonialismo en el S. XXI? Estos son algunos de los interrogantes que surgen de la lectura de los amplísimos casos de ciber espionaje en la región.

Por último, y no por ello menos importante, es necesario luchar contra los gobernantes que se comportan como "dueños" de los recursos del estado, y creen que tienen los medios suficientes para entrometerse en la vida de los particulares. Si nada garantiza la seguridad de políticos opositores a gobiernos de turno,

tampoco garantizará la seguridad digital de los ciudadanos civiles, de a pie, que muchas veces no tienen conocimiento sobre estas aberrantes situaciones.

Referencias:

Acurio del Pino, S (s/f) *Delitos Informáticos: Generalidades*. [Archivo PDF] Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Cárdenas López, A. (Marzo 2018) *"La conexión electoral del espionaje informático en América Latina: el Watergate criollo"*. Revista Globalización [En línea] Disponible en http://www.rcci.net/globalizacion/2018/fg3374.htm

"El espionaje digital tiene un efecto devastador para los derechos humanos, denuncia experta" (14 Marzo 2023) Noticias ONU. [en línea] Disponible en https://news.un.org/es/story/2023/03/1519377

"Instrumentos de espionaje y vigilancia: Aumentan las amenazas a la intimidad y los derechos humanos, advierte un informe de las Naciones Unidas." (16 de septiembre de 2022) Comunicados de Prensa. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. [en línea] Disponible en https://www.ohchr.org/es/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

Mayer Lux, L. y Vera Vega, J (diciembre 2020) "El delito de espionaje informático: Concepto y delimitación." Revista chilena de derecho y tecnología. Versión On-line ISSN 0719-2584 [en línea] Disponible en https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000200221

Bibliografía Consultada:

Corvalán, J. G (2018) *"Inteligencia artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia."* Artigos. **Revista de Investigações Constitucionais** 5 (1) [Archivo PDF] Disponible en https://www.scielo.br/j/rinc/a/gCXJghPTyFXt9rfxH6Pw99C/

Del Palacio, G (23 de junio de 2013) "¿Qué es PRISM? Todas las claves del programa de vigilancia de EEUU". Hipertextual. [en línea] Disponible en https://hipertextual.com/2013/06/que-es-prism-claves

Grigore, A.E (2022) "Derechos humanos e inteligencia artificial". Revista Ius et Scientia. Vol. 8 N° 1 ISSN 2444-8478. [Archivo PDF] Disponible en https://revistascientificas.us.es/index.php/ies/article/view/19991/18568

Iglesias Álvarez, I (03 Mayo 2022) "Pegasus, las claves del software israelí que ha puesto en jaque al Gobierno de España" CSO Computerworld. España. [en línea] Disponible en https://cso.computerworld.es/cibercrimen/pegasus-las-claves-del-software-israeli-que-ha-puesto-en-jaque-al-gobierno-de-espana

"Primer acuerdo mundial sobre la ética de la inteligencia artificial." Noviembre 2021. Derechos humanos. Noticias ONU. [en línea] Disponible en https://news.un.org/es/story/2021/11/1500522

Temperini, M.G.I (2014) Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 2da Parte. 14° Simposio Argentino de Informática y Derecho, SID 2014. [Archivo PDF] Disponible en https://43jaiio.sadio.org.ar/proceedings/SID/13.pdf

---

[1] Abogada y Procuradora egresada de la Universidad Nacional de San Luis (Argentina), sumamente interesada en las tareas de docencia e investigación, especialmente en el área de Derechos Humanos. Pasante en el Proyecto de Investigación PROICO N° 15-0120 "Derecho y lenguaje: Delimitación y Alcance de Criterios Judiciales" de la Universidad Nacional de San Luis. Pasante en la asignatura "Finanzas Públicas y Derecho Tributario" correspondiente a la carrera de Abogacía en la Facultad de Ciencias Económicas, Jurídicas y Sociales de la Universidad Nacional de San Luis. Correo electrónico: mariaagustinapuebla.5a@gmail.com