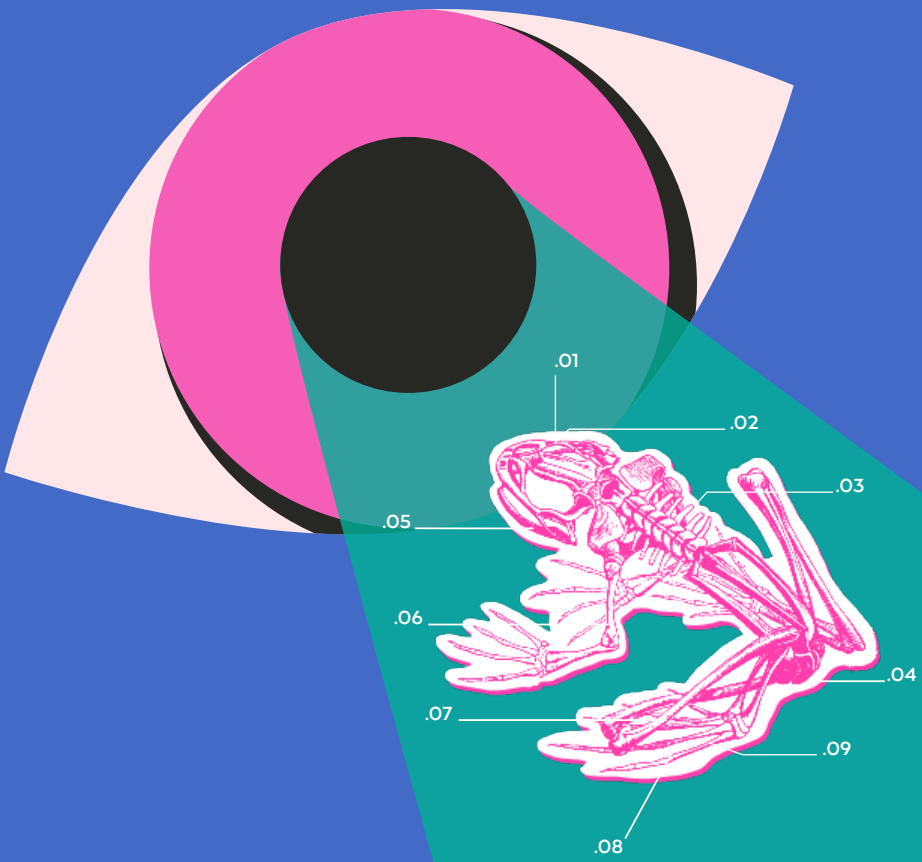
ENERO
2016

INFORME BREVE 2

VIGILANCIA EN CHILE: CONCEPTOS NORMATIVOS

PAULA JARAMILLO GAJARDO



@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina

Este informe fue realizado como parte del trabajo Derechos Digitales en la Cyber Stewards Network, en el marco de un proyecto financiado por el International Development Research Centre, Ottawa, Canada.

Derechos Digitales:
Organización No Gubernamental fundada en el año 2005, cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés están la libertad de expresión, los derechos de autor y la privacidad.

Diseño y diagramación: Constanza Figueroa
Corrección: Vladimir Garay

Enero de 2016

Introducción

Una vez conocidas cuáles son las instituciones habilitadas en Chile para ejercer actividades de vigilancia e inteligencia, incluidas aquellas vinculadas a la vigilancia de comunicaciones como hemos visto,[1] corresponde hacerse cargo del contenido de ciertas denominaciones que serán de uso frecuente en el marco de esta investigación.

Nos referimos en este punto tanto a conceptos específicos, como también a los matices que podemos encontrar entre aquellos que son de frecuente e indistinta utilización, no solo en el marco de esta investigación sino también en el diario quehacer de las agencias con impacto en la ciberseguridad en el país. Es el caso de nociones como las ya mencionadas "vigilancia" e "inteligencia" y también de aquellas orientadas al entorno digital: "cibervigilancia", "ciberseguridad" y "ciberataques", por mencionar algunas.

¿Son finalmente lo mismo? ¿Qué definición entregan las normas vigentes? ¿A qué obedecen las diferencias que podemos encontrar? ¿Cuál resulta más adecuado utilizar y en qué contexto? Dar respuesta a estas preguntas es la finalidad perseguida en esta segunda entrega, que tiene lugar en el marco del proyecto denominado "Vigilancia e Inteligencia en la agenda Latinoamericana de ciberseguridad: el caso de Chile".

1 Ver Informe Breve N.º 1.

1. En Chile

Al recurrir a fuentes nacionales de derecho para conocer qué es lo que señalan respecto a los conceptos cuyo contenido nos interesa despejar, encontramos que la ley 19.974, referida al Sistema de Inteligencia del Estado y que Crea la Agencia Nacional de Inteligencia (ANI), en su artículo 2° define dos conceptos: inteligencia y contrainteligencia.

Sobre el concepto de inteligencia, la ley chilena lo identifica como "el proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones".

En tanto, las actividades de contrainteligencia corresponderían a una porción o parte del proceso de inteligencia, con el propósito de "detectar, localizar y neutralizar las acciones de inteligencia desarrolladas por otros Estados o por personas, organizaciones o grupos extranjeros, o por sus agentes locales, dirigidas contra la seguridad del Estado y la defensa nacional".

Por otra parte, sabemos de la creación del Comité Interministerial sobre Ciberseguridad, que reúne a representantes de las principales subsecretarías del gobierno central y de la ANI. Dicha instancia ha servido para conocer la conceptualización que desde el Gobierno de Chile se maneja de ciberseguridad. Creado mediante el decreto Nº 533 (publicado el 17 de julio de 2015), en el artículo 7º dispone que "para efectos del presente decreto, se entenderá por ciberseguridad aquella condición caracterizada por un mínimo de riesgos y amenaza a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como también el conjunto de políticas y técnicas destinadas a lograr dicha condición". La definición del gobierno chileno, entonces, acude a un concepto de ciberseguridad que engloba tanto a una condición de riesgo reducido, como también a los medios para lograr esa condición, en relación con tecnologías.

Hasta esta fase del avance de la investigación en curso, no hemos logrado identificar otros cuerpos normativos que contengan definiciones que puedan ser útiles en el contexto del presente reporte. En efecto, no ha sido posible localizar una definición normativa de vigilancia o de actividades de vigilancia, ni de su contrafaz en el ciberespacio –cibervigilancia– que resulte oportuno mencionar. No obstante, el mencionado proceso de elaboración de una política nacional de ciberseguridad en Chile aparece

como una oportunidad para el planteamiento, por parte del Estado chileno, de una reconceptualización de actividades estatales vinculadas a la seguridad en el entorno tecnológico.

2. En el mundo

Si analizamos lo que se ha dicho en otras partes del mundo respecto a estas mismas nociones, nos encontramos con una definición muy gráfica provista por la Universidad de Maryland, que señala que la "ciberseguridad, también llamada seguridad informática, se centra en proteger computadores, redes, programas y datos del acceso indeseado o no autorizado, modificación o destrucción".[2] Es decir, se trata de una noción vinculada a las actividades o mecanismos de reducción de riesgos.

Por su parte, también resultan de mucha utilidad las explicaciones contenidas en el sitio web oficial del Departamento de Seguridad Nacional de los Estados Unidos, denominado National Initiave for Cybersecurity Careers and Studies (NCCIS),[3] donde se define ciberseguridad -que engloba tanto un estado de reducción de riesgos como el proceso para alcanzarlo- en los siguientes términos: "actividad o proceso, habilidad o capacidad, o estado en que la información y los sistemas de comunicación e información allí contenidos se encuentran protegidos de y/o defendidos contra el daño, uso no autorizado o modificación, o explotación".

Luego, en una definición extendida, se refiere a ella como "la estrategia, políticas y estándares relacionados con la seguridad de y las operaciones en el ciberespacio, incluyendo todo el espectro de reducción de amenazas, reducción de vulnerabilidades, disuasión, respuesta ante los incidentes de índole internacional, resistencia, y políticas de recuperación y actividades, además de la operación de redes computacionales, aseguramiento de la información, aplicación de la ley, diplomacia, milicia, y misiones de inteligencia en tanto ellas se relacionen con la seguridad y la estabilidad de la información global y las infraestructuras de las comunicaciones".

A nivel de organismos internacionales, podemos indicar que la Organización de las Naciones Unidas (ONU), a través de la Unión Internacional de Telecomunicaciones (UIT), también cuenta con una definición de

2 University of Meryland. Cibersecurity Primer, http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm (Revisado el 13 de enero de 2016). Traducción propia

.

3 National Initiative for Cybersecurity Careers and Studies, Cybersecurity Definition, https://niccs.us-cert.gov/glossary#letter_c (Revisado el 13 de enero de 2016). Traducción propia.

ciberseguridad señalando que "es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios y los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad".[4]

Por su parte, su homólogo a nivel americano, la Organización de Estados Americanos (OEA), a través de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), también se refiere a la definición de ciberseguridad desde la perspectiva de su extensión, manifestando que este "suele emplearse como un término amplio para referirse a diversos temas, desde la seguridad de la infraestructura nacional y de las redes a través de las cuales se provee el servicio de internet, hasta la seguridad o integridad de los usuarios. No obstante, desarrollos posteriores sugieren la necesidad de limitar el concepto exclusivamente al resguardo de los sistemas y datos informáticos. (...) este enfoque acotado permite una mejor comprensión del problema, así como una adecuada identificación de las soluciones necesarias para proteger las redes interdependientes y la infraestructura de la información".[5]

4 Numeral 3.2.3 de la Recomendación UIT-T X.1205 (04/2008) sobre "Aspectos Generales de la Ciberseguridad".

5 Relatoría Especial para la Libertad de Expresión, CIDH (OEA). "Libertad de expresión e Internet". Diciembre de 2013. https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf (revisado el 13 de enero)

Conclusiones parciales

En términos muy generales, es posible sostener que inteligencia y seguridad –o en este caso, ciberseguridad-, son conceptos altamente vinculados, en la medida que las labores relacionadas con la primera constituyen una herramienta que facilita conseguir los objetivos de seguridad trazados, ya sea tanto por el propio Estado como por empresas y particulares dentro del ámbito propio en que desarrollan sus actividades.

Como ha sido posible apreciar, se encuentran disponibles varias definiciones referidas a la ciberseguridad, las que, cual más cual menos, se orientan básicamente en dos direcciones: la protección de la infraestructura física (máquinas y redes) y la salvaguarda de la información que dicha infraestructura contiene (datos e interacciones). Ambas direcciones son cubiertas por el concepto, como un estado de ausencia o carencia de riesgos para esa infraestructura e información y como el proceso (incluyendo las herramientas y las capacidades) para alcanzar ese estado.

¿De qué se ha de defender a estos componentes cuando nos encontramos en el entorno digital? Inicialmente, de los denominados ciberataques, es decir, agresiones que utilizan esta infraestructura o los datos contenidos en ellos para provocar un daño, ya sea a Estados, empresas privadas o a ciudadanos individualmente considerados. Así es como, dentro de esta categoría de ciberataques, podemos mencionar los cibercrímenes o ciberdelitos, concepto destinado a designar aquellas conductas antijurídicas que se sirven de medios tecnológicos para su comisión, entre los que encontramos: estafas, amenazas, suplantaciones de identidad y actividades relacionadas con la infracción de los derechos de los menores de edad, entre otros.

Recientemente han alcanzado mayor boga otros conceptos cada vez más específicos dentro de la más amplia categoría de ciberataques, tales como ciberespionaje, ciberguerra y ciberterrorismo, para referirse a aquellos agresiones que se desplazan al ciberespacio, utilizándolo como el entorno o "territorio" en el que dichas conductas tienen lugar, con otros componentes de tecnologías de información como objetivos de tales ataques.

Ahora bien, existe otro concepto de frecuente utilización: cibervigilancia. Si bien no encuentra una definición formal en fuentes normativas que sirvan de referencia, puede ser caracterizado como aquel monitoreo efec-

tuado tanto por entes públicos (Estado), como por particulares (empresas o personas naturales individualmente consideradas), usualmente argumentado razones de seguridad, pudiendo exceder dicho objetivo, llegando incluso a lesionar derechos fundamentales, como la privacidad.

A modo de ejemplo, corresponde mencionar lo sucedido recientemente con la empresa italiana de espionaje electrónico Hacking Team[6] como paradigma de la vigilancia en entornos digitales a nivel estatal, carente de una mínima transparencia en cuanto a sus procesos más allá de la adquisición de la tecnología.

En efecto, una de las aristas más reconocidas de la cibervigilancia corresponde a la llamada vigilancia masiva, es decir, la recolección no autorizada, indiscriminada y a gran escala de datos que se ha visto enormemente facilitada por los bajos costos y gran alcance técnico que otorgan las tecnologías actualmente en uso. Este fenómeno se encuentra a su vez inmerso en aquel conocido como "Big Data", la captura y procesamiento de amplios volúmenes de información recolectada de diversas fuentes, analizada a gran velocidad, a fin de servir a los objetivos de quien lo requiera, ya sean estos políticos o económicos.

6 Ver sobre el punto las columnas de Derechos Digitales "Hacking Team: La era dorada de la vigilancia", por Claudio Ruiz, en: https://www.derechosdigitales.org/9292/la-era-dorada-de-la-vigilancia/; y "Hacking Team: Vigilancia estatal y violaciones a los derechos humanos", por Pablo Viollier y Gisela Pérez de Acha, en: https://www.derechosdigitales.org/9083/vigilancia-estatal-y-violaciones-a-los-derechos-humanos/

Bibliografía Consultada

1. Ley Nº 19.974, sobre el Sistema de Inteligencia del Estado y Crea la Agencia Nacional de Inteligencia.

2. Decreto Nº 533, publicado el 17 de julio de 2015. Crea Comité Interministerial sobre Ciberseguridad.

3. Recomendación UIT-T X.1205 (04/2008) sobre "Aspectos Generales de la Ciberseguridad".

4. "Libertad de expresión e Internet". Relatoría Especial para la Libertad de Expresión, CIDH (OEA). Diciembre de 2013,

5. Historia de la Brigada Investigadora del Cibercrimen (BRICIB). En: http://www.policia.cl/paginas/brigadas/bg-bricib/bg-bricib.htm


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina