DESCUBRIENDO LA AGENDA DE CIBERSEGURIDAD DE AMÉRICA LATINA. EL CASO DE ARGENTINA

TERCERA ENTREGA

3

La voz de los expertos

por los Derechos Civiles

Área de Privacidad

Marzo de 2016

https://adcdigital.org.ar

Índice

Descubriendo la agenda de ciberseguridad de América Latina: El caso de Argentina

Tercera entrega: La voz de los expertos*

I El proyecto

Las discusiones acerca de la Ciberseguridad se están desarrollando en contextos internacionales como el de la Organización de los Estados Americanos (OEA) y sus programas, sin participación de la sociedad civil y sin considerar la perspectiva de protección de los derechos humanos. Por su parte, estas discusiones también tienen lugar en las agendas nacionales, con temas tales como la seguridad del Estado, los mecanismos de inteligencia y las prácticas de vigilancia.

Los trabajos de investigación que han ido desarrollando ADC, Derechos Digitales y otras organizaciones civiles de la región sobre el tema, nos permite describir el siguiente escenario: las prácticas de vigilancia en el Cono Sur, especialmente aquellas ligadas a actividades de inteligencia,

*Este informe fue elaborado por el área de Privacidad de la ADC.

no están alineadas con una perspectiva amplia de derechos humanos, no tienen adecuado control y son usualmente fuente de conductas ilegales que terminan violentando derechos de los ciudadanos o debilitando el sistema democrático y sus instituciones. Esto es así pues hay países de Latinoamérica que cuentan con marcos legales que les permiten obtener información de sus ciudadanos en forma masiva y lo que es más grave, los organismos encargados de la recolección de esta información, de la interceptación de las comunicaciones, de las tareas de vigilancia y ciberseguridad son usualmente heredadas de gobiernos dictatoriales. Esta herencia por lo general implica métodos opacos, recolección desproporcionada de información, secreto excesivo, falta de transparencia y una larga experiencia en violaciones a derechos humanos que han quedado impunes.

Esta tercera entrega corresponde a una serie de tres documentos que iremos publicando con frecuencia bimestral y se enmarca en un proyecto de investigación cuyo resultado final será publicado durante la segunda mitad de 2016 y que tiene por objetivo principal determinar la existencia y contenido de la agenda de ciberseguridad en Latinoamérica, con especial foco en el caso argentino, para determinar luego su correspondencia con estándares protectorios de derechos humanos y en su caso, efectuar las sugerencias o recomendaciones pertinentes.

En la primera entrega, titulada “¿Qué entendemos por ciberseguridad?”, pusimos el foco en la definición del término a nivel global y nacional, para destacar la inexistencia de una definición a pesar de que el término “ciberseguridad” aparece mencionado en diferente normativa.

En la segunda entrega, titulada “Marco normativo”, mostramos cuál es la normativa en la que se encuentra inserto el término y sus alcances, con la finalidad de determinar el encuadre institucional de esta figura.

En esta tercera entrega, indagaremos sobre cuál es la opinión de algunos profesionales de la comunidad tecnológica respecto a las políticas, las prácticas y el marco normativo que hacen a la ciberseguridad en Argentina.

En el transcurso del trabajo realizado desde la ADC, principalmente a través de investigaciones, talleres y mesas de trabajo, hemos advertido que las distintas comunidades profesionales que hacen al ecosistema de Internet no siempre se encuentran trabajando en conjunto, o al menos con una comunicación fluida, siendo ejemplo de ello la particular dinámica entre la comunidad legal y la tecnológica.

Es por este motivo y porque entendemos que el trabajo interdisciplinario es crucial para el abordaje de estos temas, que encaramos el enfoque de este documento tratando de poner de relevancia los puntos de vista de aquellos profesionales que trabajan, directa o indirectamente, en la temática de la ciberseguridad. Este informe no pretende que las opiniones aquí descritas sean entendidas como el reflejo de una comunidad entera, sino por el contrario, como una muestra de la voz de expertos que se dedican a esta temática. Los profesionales que colaboraron en la realización de este documento son:

Mariano M. del Río: es especialista en Ciberseguridad, Compliance y Privacidad con más de 10 años de experiencia en la implementación de Programas de Seguridad de la Información y cumplimiento de las principales leyes y regulaciones en la materia en diferentes industrias. Fundador de SecureTech, empresa argentina de servicios de ciberseguridad y compliance. Colaborador de Securing The Human (SANS Institute), INCIBE y ENISA entre otros organismos. Miembro de Thiber – the cybersecurity think-tank – y del Centro de Ciberseguridad Industrial (CCI). Creador de Guías de Seguridad para empresas de servicios de salud, organizaciones sociales y periodistas.

Darío Piccirilli: se desempeña como experto en Pericias Informáticas desde 1981 en los fueros Civil, Laboral, Comercial y Penal. Es Magíster en Ingeniería de Software por el Instituto Tecnológico de Buenos Aires (ITBA) y la Universidad Politécnica de Madrid, y es doctorando en Informática por la Universidad Nacional de La Plata (UNLP). Es Director y profesor Titular de la cátedra de Pericias In-

formáticas en la Universidad Tecnológica Nacional (UTN), Director del curso de posgrado de Forensia Informática en la UNLP, y profesor de Posgrado de la Maestría de Ingeniería de Software en la UTN. Fue Asesor y Auditor Informático del Superior Tribunal de Justicia de la Ciudad de Buenos Aires.

Entrevistado R: otro de los profesionales que colaboró en este documento tiene una amplia trayectoria como asesor en el área de la seguridad de la información. Por motivos profesionales ha decidido mantener en reserva su identidad, por lo que será identificado a lo largo del documento como “Entrevistado R”.

A continuación examinaremos las respuestas que recibimos de este grupo de profesionales sobre ciertos aspectos de la ciberseguridad que hemos ido relevando en esta serie de informes.

II Volviendo a las bases: la ciberseguridad como práctica

Reflexiones sobre lo que significa la ciberseguridad

De acuerdo a Mariano del Río, la ciberseguridad “es la práctica que tiene como objetivo la protección de los activos de información tecnológicos, es decir, aquellos que se sustentan bajo un elemento TIC”. Adhiere además a la definición elaborada por la Unión Internacional de Telecomunicaciones.[1]

Por otra parte, Darío Piccirilli entiende a la ciberseguridad como el “control en la seguridad relacionada con Cloud[2] (datos públicos y privados), con

[1] Disponible en: https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

[2] Aclaración: Cloud refiere a la información en la Nube. https://es.wikipedia.org/wiki/Computacion_en_la_nube

el manejo de la gestión en la seguridad de validación de identidades y accesos. Comprende además la seguridad en la movilidad, relacionada con los riesgos que hoy día representan los dispositivos móviles. Incluye además la protección avanzada contra el fraude (comprendiendo datos, infraestructura y aplicaciones)".

Finalmente, para el Entrevistado R, la ciberseguridad "es el área de la seguridad de la información que se encarga de la protección de la información y de los recursos que se utilizan en el ciberespacio. Se vincula a la información y a los activos que intervienen en redes informáticas y especialmente, en Internet. En otras palabras, se focaliza en las amenazas a la información procesada, almacenada y transmitida a través de sistemas de información interconectados".

III La problemática derivada ante la falta de precisiones

Para Mariano del Río es urgente la implementación de una Estrategia Nacional de Ciberseguridad, "sobran los ejemplos tanto en América como en el resto del mundo, es la forma más adecuada de tratar una temática tan amplia. Debe ser Política de Estado el tratamiento de los riesgos de ciberseguridad que podrían afectar tanto al ámbito público, privado, como a la sociedad en general. Se requiere un marco amplio, actual y que aborde las temáticas que hoy forman parte de la vida cotidiana de las personas".

Darío Piccirilli agrega que "es básico contar con una definición y alcances del término [ciberseguridad]. Una falta de definición puede traer consecuencias negativas, al no quedar en claro cuáles son las fronteras del término. Pues se encuentra alcanzada una actividad que debe tener bien en claro los límites para tener regulaciones claras, completas y actualizables".

El Entrevistado R, en línea coincidente con el punto anterior, considera que “es importante contar con una definición o al menos, delimitar bien su alcance. Sin embargo, no existe consenso internacional al respecto y puede ocurrir que la definición que se adopte en las normas locales no sea la que después resulte del consenso entre países. Creo que hay que monitorear muy de cerca los avances de organismos internacionales y adherir a la que en el futuro se adopte. En cuanto a las consecuencias, entiendo que no contar con una definición acordada en la normativa puede acarrear que las partes intervinientes no tengan una noción uniforme del campo que se está regulando y como se dijo, no se delimite correctamente su alcance ni se logre convocar a todos los actores que deben participar”.

La situación descripta por los entrevistados resulta coincidente con una de las conclusiones del primer informe, que determinaba que la falta de una terminología clara, que ilumine y permita establecer alcances y limitaciones de las acciones del Estado argentino en materia de ciberseguridad, podría tener como desafortunadas derivaciones la superposición e incluso contradicción en criterios de implementación entre las diferentes reparticiones, la adopción de medidas discrecionales por parte de funcionarios de turno sin ningún tipo de control o supervisión, mantenimiento de prácticas opacas y falta de transparencia y, en definitiva, la generación de un escenario propicio para la vulneración de derechos humanos.

IV Buenas iniciativas sin continuidad

El rol del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC)

El especialista Del Río conoce detalladamente el Programa ICIC, para el cual colaboró de manera ad-honorem en la confección de documentos pertenecientes a la iniciativa “Internet Sano”,[3] uno de los cuatro grupos

[3] Disponible en: http://internetsano.gob.ar

de trabajo que fue creado por el Programa, con el fin de generar conciencia sobre los riesgos del uso de medios digitales mediante materiales educativos para el uso responsable de Internet.

“Si bien considero que las Misiones y Funciones del programa son apropiadas, creo que su ejecución ha sido deficiente. Al día de hoy, no contamos con un catálogo de las infraestructuras críticas, tampoco con una estrategia nacional de ciberseguridad. Sí se han realizado numerosos eventos. Respecto al impacto del programa en políticas públicas, creo que debido a la ausencia de una visión integral de la ciberseguridad, que generalmente se lleva a cabo a través de una estrategia nacional de ciberseguridad, no veo que se haya logrado influir a otros estratos del Estado con dicho programa”, comentó Del Río.

Durante el trabajo desarrollado para estos informes, personas cercanas a espacios del Estado en los que se lleva o se ha llevado a cabo trabajo en temas de ciberseguridad, han indicado que las normativas lanzadas eran utilizadas a modo de guía para que cada dependencia del Estado pudiera adoptar medidas vinculadas a ciberseguridad.

De manera coincidente con Del Río, el Entrevistado R considera que “es importante que en un país en el que se brindan, con cada vez mayor intensidad, servicios a través Internet, se hable de la importancia de la protección de las infraestructuras críticas de información. En este sentido, el Programa ICIC ha sido pionero. Sin embargo, no parece haber registrado avances significativos desde su creación, ni haber tenido incidencia sobre las políticas públicas y las prácticas de ciberseguridad en nuestro país. Es urgente iniciar este camino”.

V El trabajo de inteligencia como parte de la ciberseguridad

En algunos países de Latinoamérica, las discusiones sobre la ciberseguridad se han ido desarrollando en el mismo contexto que las temáticas de la vigilancia masiva y la privacidad de las comunicaciones digitales, puesto que algunos incluyen dentro de la práctica de la ciberseguridad a las actividades de inteligencia estatales como por ejemplo el caso de Colombia.[4]

En Argentina, la ciberseguridad ya comenzó a formar parte del sistema de inteligencia, mediante la creación de la Dirección Operacional de Inteligencia sobre la Ciberseguridad, dentro de la Agencia Federal de Inteligencia (AFI). Al respecto, los especialistas realizaron las siguientes observaciones.

Del Río sostiene que "Sin dudas [la ciberseguridad debe contar con una actividad de inteligencia permanente], basta con revisar las limitaciones que tienen las fuerzas de seguridad para abordar la temática de la ciberseguridad. Lamentablemente la AFI ha sido utilizada para otros fines que nada tienen que ver con brindar información de valor para combatir el crimen organizado. Hoy en día, la información que pueda surgir respecto a temáticas de ciberseguridad, es de valor para la investigación y combate de todo tipo de actividad ilícita".

Al respecto, Piccirilli considera que es importante mantener un seguimiento de estos aspectos, "pero vinculados a la defensa nacional y la protección de la intimidad de los ciudadanos".

El Entrevistado R considera que "la ciberseguridad debe estar soportada, entre otras, por actividades de inteligencia, pero éstas deben acotarse solo a los casos específicos en que sean necesarias y nunca avanzar

[4] Debate sobre Ciberseguridad y DDHH en el sector público. Octubre 2014. Fundación Karisma. Disponible en: https://karisma.org.co/impactos-del-debate-sobre-ciberseguridad-y-ddhh-en-el-sector-publico

sobre los derechos de los ciudadanos".

Una primera reflexión sobre el vínculo de la ciberseguridad y la inteligencia parecería mostrar que ambas no tienen por qué ser ajenas entre sí, si lo pensamos por ejemplo respecto a la detección de ataques a las infraestructuras críticas del Estado. Pero otra parte, es fundamental delimitar qué tipo de actividades de inteligencia se podrán realizar, evitando rotundamente la vigilancia indiscriminada de las comunicaciones y el accionar directo de las agencias de inteligencia, las cuales deben jugar como nexo, comunicando la información obtenida a partir del propio trabajo de inteligencia al ente encargado de la protección de las infraestructuras críticas, evitando convertirse en "policías digitales".

VI ¿Cuenta entonces la Argentina con una agenda de ciberseguridad?

Situación actual y desafíos a futuro

De acuerdo a la opinión del Entrevistado R, "Argentina no cuenta aún con una agenda de ciberseguridad. Se ha iniciado recientemente una nueva gestión a nivel del gobierno nacional, que parece haber abordado el tema desde distintos organismos, a partir de los decretos de estructura que han sido publicados recientemente. Es fundamental un trabajo coordinado entre estas áreas y con el sector privado, académico y la sociedad civil, en un marco de cooperación internacional y participación en foros específicos. La dimensión de los desafíos en materia de ciberseguridad emergentes del potencial que traen las tecnologías para el bienestar del país, deben ser puestos en conocimiento de las máximas autoridades, para que impulsen una agenda de ciberseguridad y propicien la obtención de recursos, así como instancias de cooperación y colaboración". Los decretos a los que se refiere el entrevistado –los cuales fueron dictados con posterioridad al cierre de nuestro segundo informe– son, por un lado, el Decreto

N° 13/16,[5] que crea –en la órbita del Sector Público Nacional– el Ministerio de Modernización, dentro del cual se crea a su vez la Subsecretaría de Tecnología y Ciberseguridad. La misma tiene a su cargo la elaboración de la estrategia de infraestructura tecnológica nacional, así como la protección de las infraestructuras críticas de información y ciberseguridad en el ámbito del Sector Público Nacional, además de dirigir y supervisar el accionar de la Oficina Nacional de Tecnologías de Información (ONTI), como algunos de sus objetivos. Por otro lado, el Decreto N°42/16,[6] creó en el ámbito de la Secretaría de Ciencia, Tecnología y Producción para la Defensa del Ministerio de Defensa, la Subsecretaría de Ciberdefensa , asignándole el objetivo de "entender en la coordinación con los organismos y autoridades de los distintos Poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructuras críticas" (el resaltado nos pertenece).

Por otra parte, Mariano del Río considera que ha existido una agenda, "pero no referida a la búsqueda del bien común, sino a intereses partidarios o bien al control de la sociedad. Se han conocido numerosos proyectos estatales de control de la opinión, espionaje y demás prácticas que difieren de lo que debería ser una agenda de ciberseguridad en una democracia. Creo que para considerar que existe una agenda, se deberían plantear escenarios de debate, incluyendo los distintos sectores, las problemáticas actuales y los riesgos a los cuales se enfrenta el ciudadano de a pie. Claro que también se requiere la formación de equipos nuevos".

Darío Piccirilli agrega que para tratar el tema de la ciberseguridad es importante trabajar con las Universidades Nacionales, "con el objetivo de asegurar el aporte de expertos adecuados y actualizados".

[5] Decreto 13/2016. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm

[6] Decreto 42/2016. Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm

VII Comentarios finales

El reporte publicado por la Organización de los Estados Americanos y Trend Micro en 2015 sobre el estado de la ciberseguridad en América,[7] que prestó especial atención al caso de Argentina, resaltó que "si bien la capacidad de Argentina para enfrentar a las amenazas cibernéticas ha mejorado considerablemente desde que se fundó el ICIC", marcó tres impedimentos que afectan a la práctica de la ciberseguridad nacional: "una falta consistente de conciencia entre los interesados de todos los niveles, problemas y preocupaciones respecto a la privacidad, y financiamiento insuficiente. Estos desafíos deben superarse si se quiere asegurar el éxito de las iniciativas de seguridad cibernética de Argentina".

Finalmente, consideramos conveniente remarcar algunos principios vinculados a la práctica de la ciberseguridad que estableció la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos en su informe "Libertad de Expresión e Internet".[8]

Por un lado, la Relatoría refirió que "la respuesta de los Estados en materia de seguridad en el ciberespacio debe ser limitada y proporcionada, y procurar cumplir con fines legales precisos, que no comprometan las virtudes democráticas que caracterizan a la red" (Párrafo 120, página 59). En tal sentido, "las políticas públicas en materia de ciberseguridad deben ser proporcionales al riesgo que enfrentan y, en cualquier caso, deben sopesar el objetivo de seguridad y la protección de los derechos fundamentales" (Párrafo 124, página 60).

A su vez, "las autoridades deben informar y rendir cuentas sobre las medidas tomadas en materia de ciberseguridad, tanto de aquellas directamente implementadas como de las que ejecutan intermediarios privados

[7] Reporte de Seguridad Cibernética e Infraestructuras Críticas de las América. Abril 2015. OEA. Disponible en: http://bit.ly/1Fn3O0u

[8] OEA. CIDH. Libertad de expresión e Internet. 31 de diciembre de 2013. Disponible en (PDF): https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

contratados por el Estado" (Párrafo 126, página 61). "Los programas oficiales y las políticas públicas de ciberseguridad deben contar con mecanismos de supervisión y control cuya instancia máxima sea un juez. De la misma manera, debe haber procedimientos de seguimiento con algún grado de participación de la sociedad civil" (Párrafo 128, página 61).

3

por los Derechos Civiles