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

SEGUNDA ENTREGA

2

Marco normativo

por los Derechos Civiles

Área de Privacidad

Enero de 2016

www.adc.org.ar

Índice

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

Segunda entrega: Marco normativo*

I El proyecto

Las discusiones acerca de Ciberseguridad se están desarrollando en contextos internacionales como el de la Organización de 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 están teniendo 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 ha venido 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, 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 así

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

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 significa 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 segunda 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?,[1] 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 esta segunda entrega, veremos cuál es la normativa en la que se encuentra inserta el término y sus alcances, con la finalidad de determinar el encuadre institucional de esta figura.

II Marco normativo

En la entrega anterior, al analizar qué se entiende por ciberseguridad, pusimos de resalto que existen tres aspectos en los que se podría dividir el enfoque de la definición, variando éstos según la finalidad de quien hace uso del término.

[1] ADC 2015. Disponible en (PDF): http://www.adc.org.ar/wp-content/uploads/2015/09/Primera-entrega-Descubriendo-la-Agenda-de-Ciberseguridad-en-Latinoam%C3%A9rica-el-caso-de-Argentina.pdf

Así hay quienes se refieren a ciberseguridad como:

- la protección o defensa de las infraestructuras de un Estado, sus redes, datos y usuarios;
- el trabajo que realizan las fuerzas de seguridad en investigación, prevención y acción contra delitos en el ámbito digital (cibercrimen);
- la actividad de vigilancia llevada a cabo por los organismos de inteligencia.

Los mencionados enfoques pueden atisbarse en los marcos normativos que analizaremos a continuación.

i Infraestructuras Críticas de Información y Ciberseguridad: evolución

a Resolución ex Secretaría de la Función Pública N°81/99: creación de la Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina (ARCERT)

La coordinación fue creada en 1999 dentro de la ex Secretaría de la Función Pública dependiente de la Jefatura de Gabinete de Ministros, en virtud de la facultad de establecer la política sobre tecnologías referidas a informática, teleinformática o telemática, multimediales y de telecomunicaciones asociadas con lo informático para el Sector Público Nacional.[2]

Esto así pues, según reza la Resolución, el Estado Nacional había logrado notables avances en la incorporación de tecnologías informáticas y de comunicaciones en sus organismos, la interconexión de éstos y el desarrollo de redes, con el consecuente incremento de la información que circulaba por las redes de la Administración Pública Nacional, además del aumento en la complejidad de la interconectividad entre redes, producido en gran medida por la utilización de Internet, por lo que resultaba necesario dotar a la Administración Pública Nacional

[2] http://www.infoleg.gob.ar/infolegInternet/anexos/55000-59999/58799/norma.htm

de un servicio de respuesta ante los incidentes que pudieran manifestarse en sus redes.

De tal suerte, alguno de los objetivos de la ArCERT fueron: promover la coordinación entre las unidades de administración de redes informáticas para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad; proponer normas; asesorar técnicamente ante incidentes de seguridad en sistemas informáticos, centralizar reportes sobre incidentes de seguridad; actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa, etc.

La ArCERT pasó, luego, a integrar el programa I.C.I.C.

b Resolución de Jefatura de Gabinete de Ministros N°580/2011: creación del Programa de Infraestructuras Críticas de Información y Ciberseguridad - I.C.I.C.

La Resolución de Jefatura de Gabinete de Ministros N°580/2011 creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (I.C.I.C.).[3]

Las razones de la creación de ese programa están explicados en los considerandos de la Resolución, que entre otras cuestiones destaca que la infraestructura digital de la que depende la utilización de las comunicación virtuales, es una infraestructura crítica y por ello imprescindible para el funcionamiento de los sistemas de información y comunicaciones, que a su vez dependen de modo inexorable del Sector Público Nacional y del sector privado.

La resolución destaca también que la seguridad de la infraestructura digital se encuentra expuesta a constantes amenazas, que en caso de materializarse pueden ocasionar graves incidentes en los sistemas de información y comunicaciones, por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas. Por ello deviene imprescindible la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del

[3] http://www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones.

Así se creó el I.C.I.C.,[4] que tiene como objetivo general la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones de todo el sector público nacional, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, así como al fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías.

A tal fin, I.C.I.C. deberá elaborar y proponer normas, colaborar con el sector privado, administrar información sobre reportes de incidentes de seguridad en el Sector Público Nacional y encausar posibles soluciones en forma organizada y unificada, establecer prioridades y planes estratégicos para liderar el abordaje de ciberseguridad, alertar sobre casos de detección de intentos de vulneración de infraestructuras críticas, coordinar la implementación de ejercicios de respuesta, asesorar técnicamente ante incidentes de seguridad reportados, centralizar reportes, actuar como repositorio, elaborar un informe anual de la situación en materia de ciberseguridad para su publicación abierta y transparente, monitorear los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como infraestructuras críticas para prevención de posibles fallas de ciberseguridad, promover concientización acerca de los riesgos que genera el uso de medios digitales, difundir información útil para incrementar los niveles de seguridad de las redes, entre otros.

Es dable destacar que para participar en el Programa los organismos interesados, sean del Sector Público Nacional, organismos interjurisdiccionales, organizaciones de sociedad civil y/o del sector privado, deben manifestar su adhesión al mismo.

[4] http://www.icic.gob.ar/

Asimismo, la Resolución establece que el I.C.I.C. no interceptará ni intervendrá en conexiones o redes de acceso privado, en cumplimiento de lo estipulado por la Ley de Protección de Datos Personales y normativa reglamentaria vigente.

El I.C.I.C. cuenta con cuatro grupos de trabajo:

1. ICIC CERT, para hacer frente a las emergencias informáticas;
2. Grupo de Acción Preventiva (G.A.P.), para la investigación y análisis de nuevas tecnologías y herramientas informáticas;
3. Grupo de Infraestructuras Críticas de Información (G.I.C.I.), para la identificación y análisis de las infraestructuras críticas del país, como son las telecomunicaciones, la energía, el petróleo, el gas y los servicios financieros;
4. Internet Sano, para la concientización de los riesgos del uso de medios digitales en el sector público nacional.

A través del Instituto Nacional de la Administración Pública (I.N.A.P.), el I.C.I.C. brinda cursos, talleres y charlas enfocadas en la estrategia de capacitación diseñada por la Oficina Nacional de Tecnologías de la Información (O.N.T.I.). En julio de 2014, por ejemplo, se llevó a cabo la capacitación titulada "Introducción a las infraestructuras críticas de información y ciberseguridad" con una modalidad de tipo virtual o a distancia, orientada a los agentes de entidades y jurisdicciones que componen el Sector Público Nacional a cargo de tareas administrativas, al personal de organismos interjurisdiccionales, al personal de organismos civiles y al personal del sector privado.

Esta capacitación se dividió en tres módulos, en los cuales, además de las bases teóricas sobre el tema (¿Qué son las infraestructuras críticas? ¿Qué se considera ciberseguridad?), se trataron los casos específicos de la Unión Europea con la Agencia Europea para la Seguridad de la Información y la Red (ENISA, por sus siglas en inglés), así como las estrategias de la ciberseguridad nacional del Reino Unido, Canadá, España, Estados Unidos y Alemania.

Al momento de su creación, la autoridad de aplicación del Programa I.C.I.C. era la Oficina Nacional de Tecnologías de Información (O.N.T.I.), dependiente de

la Subsecretaría de Tecnologías de Gestión de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros.

La O.N.T.I.[5] es la Oficina encargada de la implementación de estrategias de innovación informática de la Administración Pública, desarrolla los sistemas que son utilizados en procedimientos de gestión, fija los estándares que deben utilizar los organismos públicos cuando incorporan nuevas tecnologías, colabora con otras dependencias en la creación de portales informativos y de gestión y promueve la interoperabilidad de las redes de información de las instituciones estatales. También coordina las respuestas ante los intentos de ataque o penetración a las redes informáticas de los organismos públicos, fija los estándares de seguridad y controla que sean cumplidos en los sistemas del Estado, además de tener a su cargo implementación y control de uso de la certificación digital en el Estado, que permite tramitar electrónicamente los expedientes.

c El Decreto 1067/2015: la creación de la Subsecretaría de la Protección de Infraestructuras Críticas de Información y Ciberseguridad

El programa I.C.I.C. fue uno de los antecedentes para que en el mes de junio de 2015, el Poder Ejecutivo Nacional decretara la creación de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad, dependiente de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros, que tendrá como objetivo principal la estrategia nacional de protección de infraestructuras críticas de información y ciberseguridad.

Así lo estableció el Decreto del Poder Ejecutivo Nacional 1067/2015[6], esgrimiendo como fundamentación el perfeccionamiento de la utilización de los recursos públicos con miras a una mejora sustancial en la calidad de vida de los ciudadanos, focalizando su accionar en la producción de resultados que sean colectivamente compartidos y socialmente valorados.

Para ello estimó necesario establecer una nueva conformación organizativa de los niveles políticos, basado en criterios de racionalidad y eficiencia que posibiliten

[5] http://secretariagabinete.jefatura.gob.ar/ONTI

[6] http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247971/norma.htm

una rápida respuesta a las demandas de la sociedad, dando lugar a estructuras dinámicas y adaptables a los cambios permanentes.

Este mismo decreto estableció que el Programa ICIC pasara a depender de la Dirección Nacional de Infraestructuras Críticas de la Información y Ciberseguridad, creada dentro del ámbito de la nueva Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad.

Así se dispuso que la responsabilidad primaria de la Subsecretaría es la de entender en todos los aspectos relativos a la ciberseguridad y protección de las infraestructuras críticas, comprendiendo la generación de capacidades de detección, defensa, respuesta y recupero ante incidentes del Sector Público Nacional.

Para ello, la Subsecretaría debe llevar adelante acciones similares a las previstas para el Programa I.C.I.C., tales como y, por mencionar sólo algunas:

- Entender, asistir y supervisar en los aspectos relativos a la seguridad y privacidad de la información digitalizada y electrónica;
- Elaborar normas y estándares destinados a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas;
- Dictar la Política de Seguridad Modelo de la Información;
- Colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital con actualización constante,
- Establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.

Asimismo, la Resolución de Jefatura de Gabinete de Ministros 1046/2015[7] estableció la creación de tres direcciones y coordinaciones dependientes de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad.

[7] http://www.infoleg.gob.ar/infolegInternet/anexos/250000-254999/251022/norma.htm

Así se crearon tres direcciones, cada una a cargo de determinadas acciones. A saber: Dirección de Elaboración e Interpretación Normativa; Dirección Técnica de Infraestructuras Críticas de Información y Ciberseguridad y Dirección de Capacitación, Concientización y Difusión. Y dos coordinaciones: Coordinación de Procesos y Proyectos y Coordinación de Desarrollo e Investigación.

ii Inteligencia y Ciberseguridad

a Antecedentes. Estructura legal del Sistema Nacional de Inteligencia

La gestación y evolución del sistema de inteligencia argentino y su estructura y marco legal fueron analizados en nuestro informe "**El (Des)control democrático de los Organismos de Inteligencia en Argentina** ",[8] que invitamos a leer y puede descargar desde nuestro sitio web.

La escandalosa muerte del fiscal federal a cargo de la causa AMIA ocurrida el 18 de enero de 2015, al aparecer muerto de un tiro en la cabeza un día antes de presentarse ante el Congreso Nacional a declarar por una denuncia por él efectuada que involucraba a las más altas esferas del poder, puso en flagrante evidencia el penoso e ilegítimo funcionamiento del aparato de inteligencia del Estado y apuró una reforma de la ley de Inteligencia, que incluyó la creación de una nueva Agencia Federal de Inteligencia.[9]

La reforma mantuvo una regla que entendemos de suma trascendencia y que encuentra sustento en los artículos 18 y 19 de nuestra Constitución Nacional, en cuanto dispone que las comunicaciones, incluyendo cualquier sistema de envío de objetos o trasmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público son inviolables, excepto cuando mediare orden o dispensa judicial en sentido contrario.

[8] ADC 2015. Capítulo II.http://www.adc.org.ar/wp-content/uploads/2015/01/2015-01-23-Informe-Final-Inteligencia.pdf

[9] http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm

b El Decreto 1311/2015. La Nueva Doctrina de Inteligencia Nacional y la Dirección Operacional de Inteligencia sobre la Ciberseguridad

El 6 de julio de 2015, entró en vigencia el Decreto 1311/2015,[10] que estableció la Nueva Doctrina de Inteligencia Nacional como cuerpo doctrinario, la estructura orgánica y funcional del nuevo organismo y un nuevo régimen profesional del personal de la Agencia Federal de Inteligencia (A.F.I.).

El Capítulo I del Anexo I, al desarrollar el marco para la "Inteligencia para la Defensa y Seguridad Democráticas", establece que la inteligencia nacional es una actividad que se inscribe dentro del marco del Estado Constitucional social y democrático de derecho orientada a producir conocimientos acerca de las problemáticas –riesgos, conflictos- inscritas en la defensa nacional y la seguridad interior. La desviación de fines del sistema de inteligencia argentino motivó que se aclare que la inteligencia nacional debe velar por la protección y el cuidado de los argentinos, y no "espiarlos". Por ello el sistema de inteligencia nacional se configura como un "observatorio" abocado exclusivamente a la producción y gestión de conocimientos acerca del conjunto de problemáticas relevantes en materia de defensa nacional y seguridad interior.

Al explicitar las problemáticas que se consideran insertas en el ámbito de Seguridad Interior, refiere que éstas comprenden los fenómenos delictivos violatorios de las libertades y derechos de las personas y del Estado Constitucional social y democrático de derecho, y específicamente aquellos fenómenos delictivos complejos de relevancia federal.

A renglón seguido detalla los fenómenos delictivos complejos de relevancia federal:

1. Terrorismo y sus diferentes manifestaciones globales y/o locales, estatales y no estatales;

2. Atentados contra el orden constitucional y la vida democrática, se trate de grupos políticos y/o militares o de grupos económicos y/o financieros.

[10] http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

3. Criminalidad organizada, en particular narcotráfico, trata de personas, delincuencia económica y financiera, tráfico de armas, etc.

4. Acciones que atenten contra la **ciberseguridad**, delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes o los datos, o parte de ellos, el uso fraudulento y la difusión ilegal de contenidos. (el resaltado nos pertenece)

En el Capítulo II de la Nueva Doctrina, bajo el título "Dimensiones y Actividades de la Inteligencia Nacional" (Anexo I), se definen los alcances de la producción de inteligencia nacional, que comprende:

1. La inteligencia nacional estratégica

2. La contrainteligencia

3. La inteligencia criminal

4. La inteligencia estratégica militar

De las cuatro áreas mencionadas, la ciberseguridad aparece mencionada en el desarrollo de la inteligencia criminal. Así dice que la inteligencia criminal "comprende la producción de inteligencia referida a las problemáticas delictivas y, en particular, a aquellas problemáticas delictivas complejas de relevancia federal relativas al terrorismo, los atentados contra el orden constitucional y la vida democrática, la criminalidad organizada y los atentados contra la ciberseguridad".

Por su parte, el Anexo II del Decreto 1311/15 contiene la descripción de la "Estructura Orgánica y Funcional de la Agencia Federal de Inteligencia". En su Título II, Capítulo 4, se desarrolla la estructura operacional de inteligencia de la A.F.I., dentro de la cual se encuentran detalladas las funciones y composición de la Dirección Operacional de Inteligencia sobre la Ciberseguridad, con sede en la central de la A.F.I., en la calle 25 de Mayo N°11 de la Ciudad de Buenos Aires.

La Dirección Operacional de Inteligencia sobre la Ciberseguridad tiene a su cargo "la producción de inteligencia orientada al conocimiento de las acciones que

atenten contra la ciberseguridad en el marco de la defensa nacional o la seguridad interior, y de los grupos nacionales o extranjeros responsables de llevarlas a cabo".

La Dirección se compone a su vez por dos direcciones:

Dirección de Inteligencia Informática: que tiene a su cargo la producción de inteligencia orientada al conocimiento de las actividades relativas a riesgos y conflictos vinculados o derivados del uso de las tecnologías de la información y la comunicación, que afecten la defensa nacional o la seguridad interior, y de los grupos nacionales o extranjeros responsables de llevar a cabo estas actividades".

Dirección de Inteligencia sobre Delitos Informáticos: la producción de inteligencia orientada al conocimiento de las actividades que pudieran configurar delitos informáticos en cualquiera de sus formas y modalidades, y de los grupos nacionales o extranjeros responsables de llevar a cabo estas actividades.

La Dirección Operacional de Inteligencia sobre la Ciberseguridad "desarrolla las actividades institucionales de recolección, gestión y análisis de la información y está integrada por una dotación de oficiales y analistas de inteligencia especializados en ciberseguridad".

El ex-Director de la A.F.I. Oscar Parrilli, durante una conferencia de prensa brindada en julio de 2015 para presentar la Nueva Doctrina de Inteligencia Nacional, informó que la Dirección Operacional está encargada de "todo lo que en el mundo moderno hoy son los delitos cibernéticos, informáticos, todo lo que es la infraestructura crítica de la Argentina, que pasa por sus centrales nucleares, bancos y demás y toda la protección que se tiene que llevar adelante. En este sentido han ocurrido en los últimos tiempos noticias muy impactantes, ha sido amenazado y hackeado el parlamento alemán, han sido hackeadas instituciones de Estados Unidos, de Inglaterra, y aquí en la Argentina no teníamos una política que previera, estudiara, analizara y realizara inteligencia sobre estos temas. La hemos creado, la vamos a poner en marcha en los próximos días, y además fundamentalmente también tenemos el orgullo de decir que va a estar al frente de

este organismo un ingeniero informático argentino muy prestigiado, que viene de la actividad privada, que conoce profundamente todos estos temas y que nos va a dar una gran ayuda a todos los argentinos para evitar este tipo de amenazas y acciones que pueden afectar a la seguridad y la defensa nacional".[11]

Dado el breve período de tiempo transcurrido desde la puesta en funcionamiento de esta Dirección Operacional de Inteligencia sobre la Ciberseguridad, no es demasiada la información que hemos podido obtener en relación a la misma, sólo aquella surgida de algunas notas informativas. En una entrevista publicada el 1 de diciembre de 2015, el entonces director de la A.F.I. informó que la Dirección estaba funcionando en plena capacidad hacía poco menos de un mes y que su actividad consiste en mirar los ciberataques que suceden en el mundo, analizar en qué situación el país se podría considerar amenazado y realizar las advertencias adecuadas en los casos que sean necesarios; además de intervenir en investigaciones judiciales si la Justicia Federal lo requiere.[12]

III Comentario final

Las primeras reflexiones a las que arribamos en la primera entrega ponían el foco en la dificultad y el desafío que supone establecer una definición de ciberseguridad, como así también en las implicancias que para los derechos humanos podrían derivarse de la eventual adopción de una definición amplia o acotada.

Ante la falta de terminología clara que nos permita establecer los alcances y limitaciones de las acciones del estado argentino en materia de ciberseguridad o, mejor dicho, ante la falta de concepto, iniciamos esta identificación de la normativa vigente, con la finalidad de determinar el encuadre institucional de esta figura y así poder aproximarnos al objetivo principal de este proyecto, que es el de determinar la existencia y contenido de la agenda de ciberseguridad de Argentina.

[11] Parrilli, Oscar. Conferencia de prensa. Casa de Gobierno. 7 de julio de 2015. Disponible en: http://www.casarosada.gob.ar/informacion/conferencias/28837-conferencia-del-titular-de-la-afi-oscar-parrilli-en-casa-de-gobierno

[12] http://www.pagina12.com.ar/diario/elpais/1-287308-2015-12-01.html

2