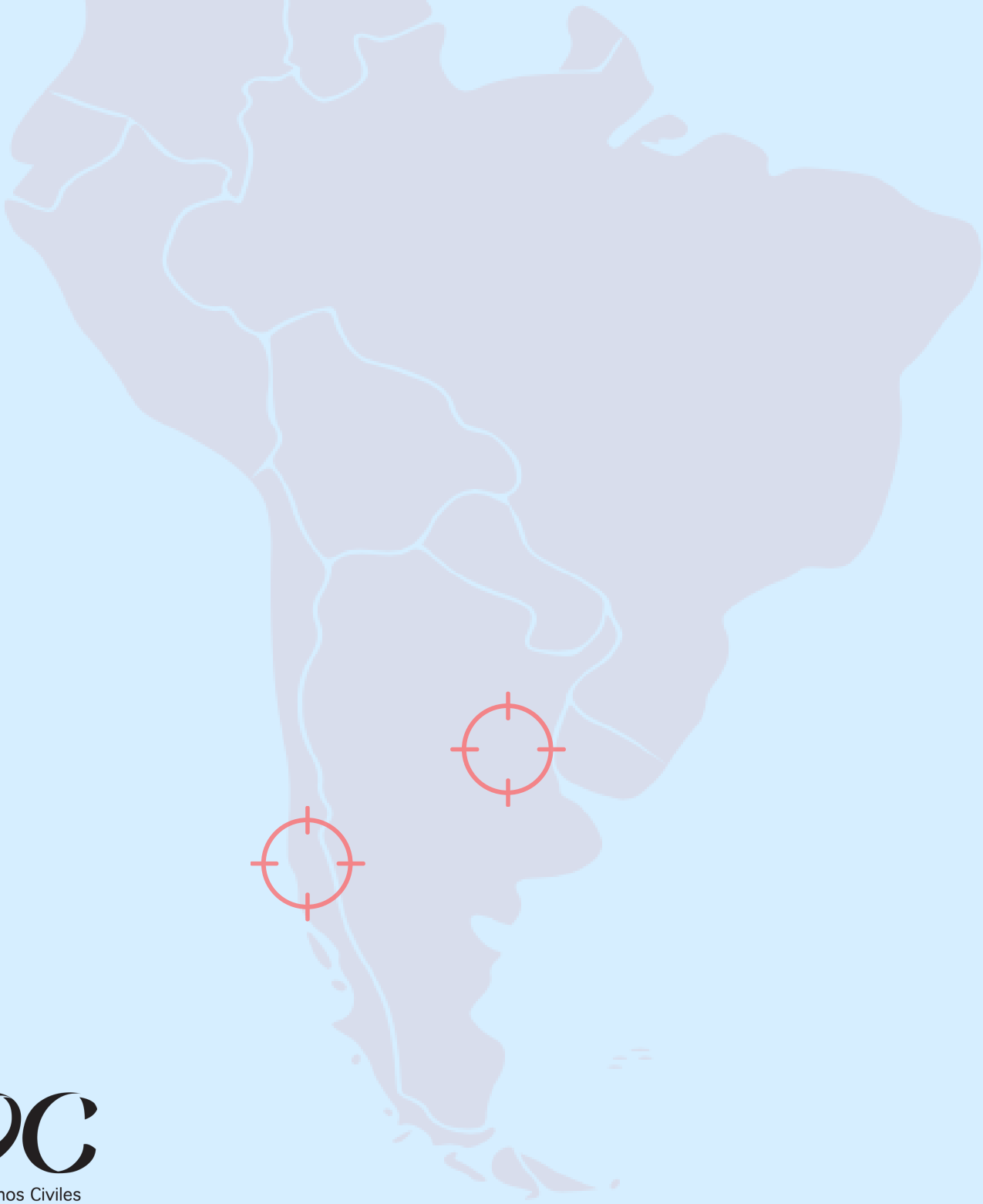
VIGILANCIA E INTELIGENCIA EN LA AGENDA LATINOAMERICANA DE CIBERSEGURIDAD

REPORTE COMPARADO: CHILE - ARGENTINA



por los Derechos Civiles

Área de Privacidad

Octubre 2016

https://adcdigital.org.ar

Vigilancia e inteligencia en la agenda latinoamericana de ciberseguridad

Reporte comparado: Chile - Argentina*

I Introducción

El presente informe es parte de un esfuerzo conjunto realizado por la Asociación por los Derechos Civiles y Derechos Digitales, y tiene como finalidad efectuar un análisis comparativo de los resultados obtenidos en investigaciones previas sobre inteligencia y vigilancia en Chile[1] y Argentina,[2] dos países claves para comprender dicho asunto a nivel latinoamericano, en el marco de un proyecto impulsado por The Citizen Lab.

El propósito mayor del proyecto es presentar los aspectos más relevantes vinculados con la ciberseguridad en el ámbito de la inteligencia y la vigilancia en línea, con una perspectiva de derechos humanos e interés público, proveniente de la sociedad civil y con miras a influir la discusión en torno a estos temas, tanto en foros nacionales como internacionales.

En estos espacios de discusión se están generando programas de ciberseguridad que, lamentablemente, carecen de participación sustantiva de la sociedad civil y de una perspectiva de derechos humanos. En el contexto latinoamericano, así ha sucedido en la Organización de los Estados Americanos (OEA) y en la discusión interna de algunos países del continente.

En este sentido, resulta interesante observar cómo ha evolucionado la discusión y la regulación sobre ciberseguridad en los países acá analizados, teniendo en consideración que comparten un pasado

*El presente documento fue elaborado por Leandro Ucciferri, abogado e investigador en las áreas de Privacidad y Libertad de Expresión de la Asociación por los Derechos Civiles, y Paula Jaramillo, investigadora y encargada de asuntos legales en Derechos Digitales.

[1] Vigilancia en Chile: hacia una Política Nacional de Ciberseguridad, Derechos Digitales, julio 2016. Disponible en (PDF): https://derechosdigitales.org/wp-content/uploads/Politica-Nacional-de-ciberseguridad.pdf

[2] Ciberseguridad en la era de la vigilancia masiva, ADC, mayo 2016. Disponible en (PDF): https://adcdigital.org.ar/wp-content/uploads/2016/06/ciberseguridad-argentina-ADC.pdf Versión en inglés disponible en (PDF): https://adcdigital.org.ar/wp-content/uploads/2016/09/Cybersecurity-Argentina-ADC.pdf

reciente marcado por el quiebre democrático y largos períodos de gobiernos dictatoriales. Esta característica ha sido capaz de dejar su impronta en la forma en que se entienden las facultades que el Estado posee para vigilar a sus ciudadanos, arrastrando un legado difícil de modificar en lo que se refiere a la perspectiva de derechos humanos (o la falta de ella), en la elaboración de políticas de vigilancia e inteligencia militar y su ulterior extensión al entorno digital.

Esta herencia conlleva carencias en cuanto a la transparencia de los métodos empleados y la desproporcionalidad en la recolección de información, que además, lamentablemente, vienen acompañadas de un historial de violaciones a los derechos humanos, en su mayoría, impunes.

El trabajo realizado en el marco del presente proyecto pretende constituir un aporte abordando la ciberseguridad no solo desde una perspectiva histórica, sino que mirando al futuro, situándose en el presente, analizando aquellos casos actuales que pueden vincularse a la temática, aún cuando se trata de un asunto cuya discusión y abordaje está en curso.

En este informe en particular, realizamos una labor comparativa en cuatro grandes áreas:

1. Existencia y contenido de un concepto de ciberseguridad tanto en Argentina como en Chile;
2. La institucionalidad u organismos a cargo de las labores vinculadas con esa actividad, incluyendo el grado de especificidad que el asunto ha alcanzado en cada uno de los países analizados;
3. La normativa vigente que se encarga de abordar las labores de vigilancia en línea o que se vinculan con ella, aunque no haga referencia específica. En este último apartado hemos incorporado la mención a lo que sucede en ambos países en materia de agenda o política sobre ciberseguridad y cuál ha sido la evolución de ese proceso en particular;
4. Y finalmente, la mención de algunos casos relevantes en ambos países que entreguen un contrapunto acerca de cómo han venido abordándose los distintos problemas que la cibervigilancia plantea cuando entra en un conflicto explícito con ciertos derechos humanos.

Por último, esta exploración conjunta decantará en una serie de recomendaciones y sugerencias que emanan de las investigaciones realizadas paralelamente.

II Conceptos

De las investigaciones llevadas a cabo en los respectivos países, surge como primera observación que la temática de vigilancia y ciberseguridad va de la mano de conceptos que en ocasiones resultan lejanos para el público general; esto conlleva una dificultad para la sociedad civil vinculada al quehacer

en derechos humanos al momento de comunicar, en términos claros y que puedan ser comprendidos por toda la ciudadanía, cómo estos impactan la vida diaria.

Esto nos llevó a analizar las normativas de cada país para comprender cómo son utilizados distintos conceptos y sus implicancias. Tanto la legislación chilena como la argentina establecen conceptos similares de lo que se entiende por inteligencia y contrainteligencia.

Respecto a la inteligencia, ambas normativas hacen hincapié en que su finalidad es obtener, sistematizar y analizar información que sea útil para conocer los riesgos y conflictos que pongan en peligro la defensa y seguridad de la Nación. Por otra parte, respecto a la contrainteligencia, ambos países destacan que debe estar orientada a evitar actividades de inteligencia que representen amenazas o riesgos para la seguridad del Estado; la normativa chilena da una definición más detallada, al remarcar quiénes son objeto de la contrainteligencia: otros estados, personas, organizaciones o grupos extranjeros o agentes locales; aclaración que no existe en la normativa argentina.

Uno de los conceptos que no cuenta con una definición en la normativa chilena ni argentina es vigilancia o "actividades de vigilancia", ni de su contrafaz en el ciberespacio, la "cibervigilancia".

En cuanto al concepto mismo de ciberseguridad, en el caso argentino pudimos concluir que, a nivel estatal, aún no hay un consenso sobre qué es ciberseguridad o una adopción unánime de su definición; pero, aún sin brindar conceptos, el término ciberseguridad aparece inserto en alguna normativa y ha sido utilizado cada vez con mayor frecuencia en los últimos años.

En Chile, la situación es rotundamente opuesta. Mediante la creación del Comité Interministerial de Ciberseguridad, que reúne a representantes de las principales subsecretarías del Gobierno central y de la Agencia Nacional de Inteligencia, se pudo conocer que la definición que adopta el Gobierno chileno sobre ciberseguridad engloba tanto a una condición de riesgo reducido, como también a los medios para lograr esa condición, en relación con tecnologías.

Al margen de la definición de ciberseguridad que pueda elaborar un país, como en el caso de Chile, las respectivas investigaciones permitieron identificar varios intentos por parte de organismos no gubernamentales por ofrecer un concepto marco de lo que es la ciberseguridad, qué implica y cómo debe ser abordada; tanto la Unión Internacional de Telecomunicaciones de las Naciones Unidas, como la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos han publicado al respecto.

III Institucionalidad

Los sistemas de inteligencia de cada país comienzan en períodos y contextos distintos, por parte de Chile sus antecedentes se remontan a la época de la Colonia, a mediados del Siglo XVIII, y a la Guerra del Pacífico, a fines del Siglo XIX; Argentina ve nacer sus servicios de inteligencia a partir de

la Segunda Guerra Mundial, en medio de una tendencia global con el afán de defender la Nación y sus intereses. Ambos países comparten un pasado oscuro, que hizo uso y abuso de los respectivos organismos de inteligencia como herramientas para violar sistemáticamente los derechos humanos de la población.

En Chile, durante la dictadura cívico-militar liderada por Augusto Pinochet se crearon organismos de inteligencia que pertenecían a alguna rama de las Fuerzas Armadas o al Cuerpo de Carabineros. El primero fue el Servicio de Inteligencia Militar, que actuó durante la preparación del golpe de Estado y hasta principios de 1974; las demás ramas de las Fuerzas Armadas también contaban con servicios de inteligencia, así se encontraban el Servicio de Inteligencia Naval, el Servicio de Inteligencia de Carabineros y el Servicio de Inteligencia de la Fuerza Aérea.

El Servicio de Inteligencia Militar fue reemplazado por la Dirección de Inteligencia Nacional (DINA), una policía secreta directamente ligada a la Junta de Gobierno, que no estaba sujeta a controles y contaba con facultades para detener, torturar, extraer información bajo apremios y confinar personas en sus centros operativos durante los estados de excepción.

En Argentina, el principal organismo de inteligencia nacional, la ex Secretaría de Inteligencia del Estado (SIDE) –actual Agencia Federal de Inteligencia–, fue regulada durante años mediante decretos secretos del Poder Ejecutivo, hasta que se sancionó la Ley de Inteligencia Nacional, con el fin de definir las actividades de inteligencia, delimitar los campos de acción e imponer mecanismos de control. La SIDE estuvo estrechamente vinculada a las dictaduras que gobernaron la Argentina durante las décadas del 50 y el 70, cumpliendo tareas de inteligencia interna bajo la dirección de los militares y en coordinación con las divisiones de inteligencia de las distintas fuerzas armadas, llegando incluso a manejar directamente un centro clandestino de detención.

La actual estructura del sistema de inteligencia chileno está constituida por organismos que pueden encuadrarse en tres categorías: a) inteligencia política: a cargo de la Agencia Nacional de Inteligencia (ANI), dependiente de la Presidencia de la República; b) inteligencia policial: en la que se encuentra la Dirección de Inteligencia Policial de Carabineros y la Jefatura Nacional de Inteligencia Policial; y c) inteligencia militar: a cargo de la Dirección de la Defensa del Estado Mayor de la Defensa Nacional y las Direcciones de Inteligencia de las Fuerzas Armadas. En los dos primeros casos, los mencionados organismos dependen jerárquicamente del Ministerio de Interior y Seguridad Pública; en el último, su vinculación al poder ejecutivo tiene lugar a través del Ministerio de Defensa Nacional.

En Argentina, el Sistema de Inteligencia Nacional está compuesto por: a) La Agencia Federal de Inteligencia, como órgano superior y director del resto de los organismos. Responde directamente al Poder Ejecutivo; b) La Dirección Nacional de Inteligencia Criminal, dependiente de la Secretaría de Seguridad Interior del Ministerio de Seguridad, como superior jerárquico de las áreas de inteligencia criminal de la Policía Federal, Gendarmería Nacional, Prefectura Naval, Policía de Seguridad Aeroportuaria y de inteligencia penitenciaria del Servicio Penitenciario Federal; y c) la Dirección Nacional

de Inteligencia Estratégica Militar, dependiente del Ministerio de Defensa, como superior jerárquico de las áreas de inteligencia de las Fuerzas Armadas.

En el contexto de las investigaciones penales, en ambos países los organismos encargados de realizar labores de vigilancia y seguridad online son las unidades especializadas de las Fuerzas de Orden y Seguridad.

En Chile encontramos entonces a la Brigada Investigadora de Cibercrimen, dependiente de la Policía de Investigaciones, y al Departamento de Organizaciones Criminales, dependiente de los Carabineros. Tanto Carabineros como Investigaciones se vinculan al Gobierno central a través del Ministerio del Interior y Seguridad Pública.

En Argentina, tanto la Policía Federal, con jurisdicción nacional, como la Policía Metropolitana, con jurisdicción en la Ciudad Autónoma de Buenos Aires, cuentan con divisiones especializadas en delitos tecnológicos; en el ámbito del Ministerio Público Fiscal, encontramos la Unidad Fiscal Especializada en Cibercrimen y en el ámbito de la Ciudad Autónoma de Buenos Aires, a la Fiscalía Especializada en Delitos Informáticos.

Una diferencia sustancial se da respecto a la institución encargada de la formulación de políticas públicas relacionadas con la ciberseguridad. A diferencia de Argentina, Chile ha comenzado a transitar formalmente el camino a la elaboración de una Política Nacional de Ciberseguridad, en la cual se han identificado una serie de organismos que tienen participación: el Departamento de Crimen Organizado de la División de Estudios y la División Informática, ambas pertenecientes al Ministerio del Interior, a lo cual se suma la colaboración de la Subsecretaría de Defensa del Ministerio de Defensa, y los Ministerios de Transporte y Telecomunicaciones; Economía, Fomento y Turismo; Relaciones Exteriores; Secretaría General de la Presidencia; la Universidad de Chile; el Instituto Nacional de Normalización; el Ministerio Público y el Poder Judicial.

Sin embargo, en Argentina se tomaron una serie de medidas dispuestas a reorganizar parte de la estructura de los distintos ministerios, a partir del cambio de administración y la llegada de nuevas autoridades al Estado Nacional. Entre esos cambios se encuentra la creación del Ministerio de Modernización, dentro del cual se establece a su vez la Subsecretaría de Tecnología y Ciberseguridad.

Este es el organismo central que coordina a las distintas dependencias estatales que venían trabajando en torno a la ciberseguridad, encontrándose esta subsecretaría a cargo de la Oficina Nacional de Tecnologías de Información (ONTI), la Dirección Nacional de Infraestructura Tecnológica y Operaciones y la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad. De esta forma, la Subsecretaría se convierte en la responsable de la elaboración de la estrategia nacional de ciberseguridad, con la facultad de coordinar al resto de los organismos que deben colaborar en el desarrollo de la misma.

IV Marco regulatorio

En este apartado del reporte conjunto nos referimos a los descubrimientos comparados que quedan de manifiesto en los rasgos generales de la normativa vigente de ambos países, así como en las agendas o políticas nacionales sobre ciberseguridad.

En cuanto al primer aspecto, corresponde destacar que una de las diferencias palpables entre la normativa argentina y la chilena corresponde a la orientación que cada una de ellas tiene. En el caso argentino, la normativa está claramente enfocada hacia asuntos orgánicos o de institucionalidad de la ciberseguridad, más que hacia los de naturaleza sustantiva, como sucede más marcadamente en el caso chileno.

Esta percepción, en el caso argentino, incluso se vio refrendada en el curso de la investigación respectiva, por lo indicado por uno de los entrevistados, el especialista Iván Arce:

"Los esfuerzos que hubo en los últimos años, desde el punto de vista institucional, son un paso en la dirección correcta, pero aún falta, falta estructurar eso en una estrategia nacional, cubrir los agujeros y los baches conceptuales, delimitar y agregar lo faltante. [La ciberseguridad] no es un tema solo de seguridad, defensa e inteligencia; son varias cosas más, aspectos económicos, sociales y comerciales. Faltan cuestiones regulatorias, cuestiones de desarrollo tecnológico, de tener un ecosistema sustentable de ciberseguridad. Hay que pensarlo en forma holística ".

En ese sentido, cabe destacar que se ha logrado un grado de especialidad de los órganos a cargo de las labores de ciberseguridad que, a simple vista, parece ser mayor que el existente en Chile. En este último, el foco ha estado puesto en el otro extremo: las normas de fondo más que la creación de los órganos encargados de ellas.

De esto queda clara evidencia al comprobar que el ordenamiento contiene normas referidas a la protección de la privacidad desde la Constitución y hasta llegar a normas mucho más específicas sobre vigilancia y ciberseguridad, particularmente relacionadas con la protección del mencionado derecho fundamental en contextos tales como el procedimiento investigativo penal, telecomunicaciones, acceso a la información pública, vigilancia en espacios públicos y privados, por mencionar algunos.

Sin embargo, en cuanto a la creación de órganos especializados encargados de esta materia, es claro que existen asuntos pendientes: a la fecha solo se ha creado un comité interministerial encargado de la elaboración de una política nacional de ciberseguridad, mientras que los restantes órganos tienen competencias genéricas en materia de seguridad y vigilancia, a las que han incorporado labores propias del ciberespacio. Incluso expresamente se ha dejado constancia de la necesidad de fortalecer el centro de respuesta ante incidentes (CSIRT-CL), tanto en reportes internacionales como en la propuesta de una política nacional de ciberseguridad.

En otra arista del asunto relacionado con la normativa destinada a la protección de los datos personales en ambos países, también surge otra diferencia palpable: mientras en Chile esta materia trae a la memoria una cantidad de procesos modificatorios fallidos, que dan como resultado una ley vigente sobre protección de datos de entre las más carentes a nivel latinoamericano, en Argentina el problema discurre por otro lado, pero lamentablemente, en ambos casos, decanta en resultado negativos que finalmente resultan asimilables. En efecto, Argentina reconoce que los estándares legales de protección de la privacidad, en particular de los datos personales, es alto, siguiendo un modelo regulatorio de corte europeo. Sin embargo, el talón de Aquiles estriba en la prohibición de procesar y transferir datos personales sin el consentimiento del titular de los datos, regla que no aplica cuando se trata de bases de datos de organismos estatales.

Así, la amplitud en la redacción de la norma permite que distintos organismos estatales puedan tratar datos personales más allá de lo proporcional y estrictamente necesario. Como consecuencia, las labores de cibervigilancia efectuadas por el Estado se ven facilitadas en desmedro de la necesaria protección de los derechos fundamentales.

En cuanto a la existencia de una agenda nacional o política de ciberseguridad, podemos señalar que Chile lleva la delantera, existiendo ya una propuesta concreta, de público conocimiento, que ha sido objeto de consulta entre la ciudadanía y que debería, próximamente, concretarse en la publicación de una política formal.

En suma, el proceso ya se encuentra en curso, no obstante, los reparos que se le puedan formular a la propuesta, que a grandes rasgos apuntan a su excesiva amplitud y falta de profundidad en el abordaje de los temas que la componen, tal como hemos referido en los reportes previos.

En tanto en el caso argentino, si bien han existido anuncios públicos en torno a la elaboración -y derechamente, a la adopción- de una futura política pública, los hallazgos de los informes previos dan cuenta de que ello no ha llegado a materializarse. En este sentido, el desempeño del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) no ha sido, en absoluto, el esperado, en la medida que ha trabajado de espaldas a la ciudadanía y no ha elaborado ni publicado los productos que resultaban esperables.

El fenómeno anterior responde a varias causales, entre las que también se encuentra la falta del presupuesto necesario para dar cumplimiento a los objetivos trazados inicialmente y la falta de lineamiento de su actuar como una política de largo plazo.

En defecto de una política de ciberseguridad, en el caso argentino se ha avanzado a través de iniciativas como "Internet Sano" de ICIC y "Con Vos en la Web" de la Dirección Nacional de Protección de Datos Personales. Si bien ambas fueron bien recibidas y consideradas un aporte en cuanto a la capacitación en tecnologías y derechos humanos, hoy se encuentran cerradas, sin noticias de su posible continuidad.

V Ciberseguridad y vigilancia: casos

En ambos países se han presentado casos vinculados a ciberseguridad que pueden ayudar a dar una mirada concreta sobre la forma en que se manifiesta la vigilancia en el ciberespacio en América Latina. La mayoría de estos casos han surgido y se han desarrollado a través de la prensa, sin la seriedad que pudieren haber detentado de existir formalmente una política de ciberseguridad vigente, desde una perspectiva de los derechos humanos involucrados en ellos. En Argentina, resulta interesante constatar que la única información revestida de mayor formalidad proviene del reporte "Seguridad Cibernética e Infraestructura Crítica en las Américas", del año 2015 y elaborado por Trend Micro Inc. en conjunto con la OEA; no obstante, la conclusión que emana a partir de esa información no genera sino más dudas.

En el informe se hace referencia a la labor del ICIC colaborando en la aprobación de legislación relacionada con el cibercrimen y facilitando con ello la "investigación y persecución exitosas de varios casos de criminales cibernéticos", sin entregar mayores señas de casos concretos para su identificación.

En tanto en Chile, hemos recopilado casos que datan de hace ya varios años, en muchos de los cuales Derechos Digitales ha tenido directa participación realizando labores concretas para lograr la corrección de algunas conductas anómalas de vigilancia, provenientes de órganos encargados de la investigación y persecución de delitos, con resultados diversos.

Resulta impactante constatar cómo estos hechos han afectado a etnias, como el pueblo mapuche, y a estudiantes universitarios, cuyos derechos se han intentado conculcar vulnerando su privacidad en redes sociales. El alcance de las conductas de vigilancia lesivas de derechos que han alcanzado el ciberespacio, en una sociedad democrática y un estado de derecho, parecen ir en franco aumento.

Incluso los intentos en esa dirección, en el caso particular de Chile, quedan de manifiesto en los numerosos proyectos de ley que buscan regular actividades que tienen lugar en la red o involucran el uso de tecnología, coartando de paso derechos fundamentales.

El último ejemplo de ello, y a modo de actualización en la información plasmada en el reporte final del caso chileno, dice relación con el fallo emanado de la Corte Suprema a principios del mes de junio de 2016, resolviendo en definitiva la suerte de los globos de televigilancia instalados en dos comunas de la capital. En la sentencia, la Corte finalmente permitió que las cámaras instaladas en estos dispositivos continúen en funcionamiento, aunque reconociendo abiertamente que ellas sí lesionan la privacidad de los habitantes e impuso algunas condiciones para su operación (las que, analizadas por Derechos Digitales, resultan poco ajustadas a la realidad).[3]

Finalmente, no podemos dejar de mencionar el que probablemente sea el caso más relevante y sonado de los últimos años, relacionado con vigilancia en el ciberespacio y que ha cruzado a todo el

[3] Sobre el particular: http://bit.ly/2dXQHgC

continente latinoamericano. Se trata del caso vinculado a la empresa italiana de malware "Hacking Team", que comercializa software para espiar y acceder remotamente a dispositivos electrónicos. Paradójicamente, la empresa fue hackeada y sus relaciones comerciales con distintos gobiernos fue expuesta. En el caso argentino, su influencia llegó sólo al nivel de tratativas, con miras a un potencial negocio. Sin embargo, en los reportes preliminares de esta investigación se informó como un hecho conocido la presencia de otra empresa distribuidora de software de interceptación de comunicaciones y vigilancia en ese país: la norteamericana Blue Coat.

Por su parte, Chile fue develado como cliente de la empresa italiana, haciéndose de público conocimiento que la Policía de Investigaciones había adquirido su software a cambio de una importante suma de dinero. Esta compra se realizó con dineros públicos y en secreto. A la fecha no ha sido posible conocer las condiciones en que se ha utilizado esta tecnología ni quiénes son los ciudadanos vigilados, no obstante, se ha asegurado que se da cumplimiento a todos los requerimientos legalmente exigidos.

Analizado el caso en un extenso informe elaborado por Derechos Digitales, se ha llegado a la conclusión de que, aún cuando fuere efectivo que se da cumplimiento a la ley al momento de operar este malware, ello podría resultar insuficiente considerando la amplitud y contexto en que fueron creadas las normas legales habilitantes para ejercer la vigilancia, ya sea con fines de inteligencia o de investigación penal, que no fueron pensadas específicamente para una plataforma tecnológica, pudiendo vulnerar no solo la privacidad del sujeto directamente vigilado, sino también indirectamente la de sus contactos.

VI Conclusiones y recomendaciones

Ante la falta de consensos internacionales en cuanto a las definiciones y límites de la ciberseguridad, América Latina aún se encuentra a tiempo de avanzar hacia una nueva definición que no sea de corte exclusivamente militar ni derivada del lenguaje de inteligencia, sino que se enmarque en el reconocimiento y respeto por los derechos fundamentales y los estándares internacionales de derechos humanos.

Si bien se han realizado estudios a nivel regional sobre el estado de la ciberseguridad en distintos países latinoamericanos, es imprescindible remarcar la necesidad de contar con más análisis, idealmente realizados por grupos de trabajo locales y no por organismos internacionales que sólo se hacen eco de respuestas de organismos estatales y, de esta forma, ayudar en la construcción de políticas que ayuden a generar un ecosistema de ciberseguridad saludable. Es fundamental poder evaluar el panorama para actuar en consecuencia.

En Argentina, las iniciativas de los últimos años en el campo de la ciberseguridad aparentemente iban en la dirección correcta, intentando focalizar el trabajo desde el Estado, a través de objetivos y tareas

que resultaban adecuados para el desarrollo de una agenda de ciberseguridad. En la práctica, esto no ocurrió. Chile muestra un panorama más desarrollado desde un punto de vista normativo. Pero el estado de la ciberseguridad en Chile aún carece de suficiente madurez, en donde la propuesta de una política nacional de ciberseguridad (PNCS) pretendió abarcar un gran número de temas, lo que terminó por lograr que esta no cuente con una profundidad o dirección que resulte lo suficientemente clara, intentando suplir otras carencias de políticas públicas en otras áreas relacionadas.

Una diferencia sustancial entre ambos países es el modo en que se ha abordado la ciberseguridad. Mientras que en Chile se optó por un proceso de cara a la ciudadanía, a través de la participación en una consulta abierta, en Argentina el abordaje de la ciberseguridad desde el Estado se ha caracterizado por la falta de transparencia, tanto de sus acciones, tareas y resultados, como en la marginación de la comunidad técnica y la sociedad civil de la discusión, al no contar con un modelo de múltiples partes interesadas que pueda aportar una visión más amplia que tienda a mejorar las políticas propuestas.

Aún así, en ambos países es necesario que se produzca un debate abierto sobre la vigilancia y la ciberseguridad a nivel nacional, que involucre a todos los actores de la sociedad, para asegurar un pleno desarrollo de políticas públicas que cuenten con una mirada necesariamente holística y que alcance a todos los estratos de la sociedad, a la vez que sirva con el fin de generar una cultura social de mayor conciencia en torno a la importancia de la privacidad.

En consecuencia, a partir del trabajo conjuntamente realizado es posible formular las siguientes recomendaciones:

- Es necesario consensuar los elementos o ejes en función de los cuales se debería abordar o ceñir la definición de ciberseguridad desde una perspectiva regional, tomando en consideración el historial latinoamericano de quiebres democráticos que suelen asociar dicho concepto con labores de inteligencia y vigilancia militar. Sobre el punto es preciso procurar que se amplíe esa visión, dotándola de una adecuada perspectiva de derechos humanos.

- Incentivar el desarrollo de más estudios sobre ciberseguridad desde y para Latinoamérica, que consideren tanto los aspectos institucionales como normativos involucrados en cada uno de los países de la región.

- Realizar acciones tendientes a abrir el debate acerca de la ciberseguridad a la ciudadanía y la sociedad civil, recogiendo sus inquietudes y opiniones como parte del proceso de formulación de una política o agenda de ciberseguridad nacional y su evaluación posterior.

A través de las respectivas investigaciones se pudo concluir que tanto Chile como Argentina colocan el debate sobre la ciberseguridad en la agenda pública como parte de una tendencia internacional y no por una necesidad real, evaluada y concreta a la que hacer frente, lo que se traduce en que, aún

desde los respectivos Estados, no hay una idea acabada de cómo abordar o desarrollar correctamente el tema, problema que requiere de una pronta solución.

Finalmente, es menester mencionar que, a comienzos de abril 2016, un conjunto de organizaciones de la sociedad civil latinoamericana, entre las que se encuentran Derechos Digitales y la Asociación por los Derechos Civiles, firmamos una declaración sobre seguridad digital que establece diez puntos fundamentales que entendemos deben ser impulsados localmente en nuestros países con el fin de alinear las políticas de ciberseguridad con una perspectiva de derechos humanos.[4]

[4] Declaración de sociedad civil latinoamericana sobre seguridad digital, abril 2016, disponible en: https://adcdigital.org.ar/2016/04/06/oea-declaracion-sociedad-civil-latinoamericana-seguridad-digital/


por los Derechos Civiles