PRIVACY INTERNATIONAL

Comité de Derechos Humanos, 117° Sesión, 27 de Junio- 22 de Julio 2016

El derecho a la privacidad en Argentina

Comunicación conjunta de la Asociación por los Derechos Civiles y Privacy International previa al examen de la República Argentina, Comité de Derechos Humanos, 117° Sesión

27 de Junio- 22 de Julio 2016

PRIVACY INTERNATIONAL

ADC por los Derechos Civiles

1. Introducción

La Asociación por los Derechos Civiles (ADC) y Privacy International toman nota de las respuestas del gobierno de Argentina a la lista de cuestiones antes de la presentación del informe, en particular en relación a la legislación, políticas y prácticas relacionadas con la vigilancia y la protección de los datos personales.[1]

Privacy International es una organización de derechos humanos que trabaja para favorecer y promover el derecho a la privacidad y la lucha contra la vigilancia en todo el mundo. La Asociación por los Derechos Civiles (ADC) es una ONG independiente creada en 1995 con sede en Buenos Aires, comprometida con la promoción del respeto a los derechos humanos en Argentina y América Latina.

Las organizaciones tienen preocupaciones actuales relacionadas con el respeto al derecho a la privacidad y a la protección de datos personales en Argentina. En esta presentación, las organizaciones proporcionan al Comité información adicional y actualizada a aquella contenida en la exposición presentada al Comité antes de la adopción de la lista de cuestiones previas a la presentación del informe en Diciembre de 2013.[2]

2. Vigilancia de las comunicaciones

Según la ley de Inteligencia Nacional[3], la vigilancia de comunicaciones privadas puede ser llevada a cabo sólo si una orden judicial es dictada específicamente para el caso en cuestión. Hasta Diciembre de 2015, el único órgano estatal que estaba legalmente autorizado para levar a cabo la vigilancia de las comunicaciones era el Departamento de Interceptación y Captación de las Comunicaciones (DICOM) bajo la órbita del Ministerio Público[4], pero mediante el decreto N° 256/15 el Poder Ejecutivo transfirió la DICOM a la órbita de la Corte Suprema,[5] la cual reemplazó posteriormente a la DICOM por la Dirección de Captación de Comunicaciones, (DCC).[6] La DCC va a ser conducida por un juez, designado mediante sorteo, por el lapso de un año.

1 Ver ONU doc. CCPR/C/ARG/5, 13 Julio 2015.
2 Disponible aquí: http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/ARG/INT_CCPR_ICS_ARG_16054_E.pdf
3 Ley Nº 25.520, art. 5, http://bit.ly/1bp2vWp
4 Ley Nº 27.126, art. 17, http://bit.ly/1CLiBGU
5 Decreto Nº256/15, http://bit.ly/1RI8wLr
6 “La Corte Suprema creó la Dirección de Captación de Comunicaciones del Poder Judicial” Centro de Información Judicial Febrero, 2016, http://bit.ly/1Urvf5d

En Febrero de 2016, ADC manifestó su preocupación respecto a ciertos aspectos relativos a la creación de la DCC. De especial preocupación es el término de duración del mandato del director de la DCC, que es de sólo un año. Esta duración no brinda suficiente tiempo al juez designado para llegar a conocer cómo funciona el sistema, teniendo en cuenta que el conocimiento del sistema de interceptación de comunicaciones no es un prerrequisito para los jueces.[7]

Además, las agencias de inteligencia en Argentina operan con una gran autonomía y con poco control efectivo de sus actividades. Los últimos años han visto cambios significativos en la organización de los servicios de inteligencia en Argentina. En julio de 2015, el decreto 1311/2015 presentó la Doctrina de Inteligencia Nacional, dando un marco legal a la Agencia Federal de Inteligencia, respecto a la estructura funcional y orgánica de la nueva Agencia, así como un nuevo régimen profesional para sus agentes.[8]

Sin embargo, con el cambio de administración luego de las elecciones presidenciales, en Mayo de 2016 el decreto 656/16 derogó la estructura establecida en la Doctrina de Inteligencia Nacional y facultó al director de la agencia de inteligencia a aprobar su propia estructura organizacional y a dictar reglas complementarias y aclaratorias. Esto podría conducir a la creación de una nueva estructura organizacional bajo absoluto secreto, ya que el decreto no exige que sea público, lo cual podría significar un gran retroceso en el proceso de democratización del sistema de inteligencia.[9]

Aunque hay poca información disponible sobre las prácticas de vigilancia y las capacidades técnicas de las agencias de inteligencia, continúa la preocupación de que la vigilancia sea llevada a cabo de formas que viole el derecho a la privacidad de los individuos. De especial preocupación son los informes de ataques contra políticos, periodistas y otros activistas. El 8 de diciembre de 2015, Citizen Lab –de la Universidad de Toronto- publicó "Packrat: Siete Años de un Actor de Amenaza en América del Sur", un informe de investigación que exhibía un uso intensivo de malware, phishing y una campaña activa de desinformación en varios países latinoamericanos, incluyendo Ecuador, Argentina, Venezuela, y Brasil.[10] Respecto a Argentina, Citizen Lab mencionó ataques a figuras políticas en ataques con malware, tales como el fallecido fiscal Alberto Nisman y el periodista Jorge Lanata.

El 20 de Octubre de 2015, las ex diputadas Laura Alonso y Patricia Bullrich presentaron una denuncia por presunto espionaje ilegal sobre periodistas,

7 "Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones", Febrero 2016, https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-de-comunicaciones/

8 ADC investigó acerca del entrenamiento impartido a los agentes de inteligencia durante 2015, en su informe "Educar para vigilar", Diciembre 2015, https://adcdigital.org.ar/wp-content/uploads/2016/01/Educar-para-vigilar.pdf

9 A comienzos de 2016, el gobierno designo un nuevo Director y Vice Director de la Agencia Federal de Inteligencia (AFI)), Gustavo Arribas and Silvia Majdalani, respectivamente. ADC, junto con otras organizaciones, manifestó su preocupación sobre la falta de entrenamiento y experiencia en asuntos de inteligencia de los funcionarios designados, lo cual pone en cuestión su capacidad profesional para tan sensibles posiciones. Savoia, Claudio. "La interna de la ex Side arde con las designaciones polémicas", Clarín, 19 de diciembre de 2015. Disponible en: http://www.clarin.com/politica/Agencia_federal_de_Inteligencia_0_1489051101.html "ICCSI: Problemas en la designación de autoridades de la AFI", 30 de marzo de 2016. Disponible en: https://adcdigital.org.ar/2016/03/30/iccsi-problemas-designacion-autoridades-afi/

10 John Scott-Railton, Morgan Marquis-Boire, Claudio Guarnieri, and Marion Marschalek, "Packrat: Seven Years of a South American Threat Actor", Citizen Lab, Diciembre, 2015, http://bit.ly/1U3dFkI

políticos, fiscales y jueces, llevadas a cabo por la Agencia Federal de Inteligencia.[11] La denuncia fue rechazada por falsa por el ex Ministro de Defensa Agustín Rossi, y el ex Director de la AFI, Oscar Parrilli. Desde su presentación, no ha habido nuevos desarrollos alrededor del actual estado de la causa y la investigación sobre la presunta interceptación ilegal de las comunicaciones.

3. Régimen de protección de datos

Argentina posee fuertes estándares de privacidad, arraigados en la Constitución, así como legislación sobre protección de datos que se comparan a las de Europa, aunque la capacidad de la Dirección Nacional de Protección de Datos Personales para hacer cumplir la ley de protección de datos personales ha sido cuestionada.[12]

La ley N° 25326 (de regulación de la protección de datos personales) sigue estándares internacionales, y se aplica al procesamiento de datos personales por órganos públicos y privados. Sin embargo, la ley, en gran medida, no se aplica en la práctica. El marco legal protectorio tiene dos debilidades estructurales.

- una excesiva tolerancia en favor del Estado, en lo concerniente al almacenamiento, procesamiento, y transferencia de datos personales; y
- un órgano de contralor débil, que depende del poder ejecutivo.

Tratamiento de datos personales por autoridades estatales

En cuanto a la primera cuestión, la ley 25.326 protege los datos personales incluyendo la prohibición de procesar y transferir datos personales sin el consentimiento del titular de los datos.[13] Esta prohibición busca impedir el uso no autorizado de datos personales al dotar a los individuos con la facultad de impedir a terceros que usen sus datos personales para fines no autorizados por ellos.

Sin embargo, este principio, que es la base de la protección de los datos personales, no está presente en gran medida, cuando se trata del Estado.

El artículo 5 de la ley exige el consentimiento para el procesamiento de datos personales pero establece que el mismo no será considerado necesario cuando los datos "se recaben para el ejercicio de funciones propias de los poderes del Estado". Esto significa que la garantía del consentimiento no es útil cuando los datos son recolectados por el Estado.

De manera similar, el artículo 11 prohíbe la cesión de datos personales si el

11 "Denuncian espionaje de la Secretaría de Inteligencia a jueces, políticos y periodistas" , La Nación, Octubre, 2015, http://bit.ly/1OGTcm2 "Denuncian que el Gobierno hizo espionaje ilegal sobre políticos, jueces y periodistas" , Clarín, Octubre, 2015, http://clar.in/21RuOzZ
12 "El estado recolector" Asociación por los Derechos Civiles, Septiembre, 2014,
13 Ley 25326, Artículos 5.1 y 11.1.

titular de los datos no ha consentido previamente a ello. Sin embargo, esta garantía puede ser dejada de lado cuando una ley así lo establezca, cuando la cesión de los datos tiene lugar directamente entre dependencias de los órganos del Estado en la medida de sus competencias correspondientes.[14]

El art. 23 de la ley establece una regulación diferente para los bancos de datos personales de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia, de acuerdo a la finalidad para la cual fueron creados. El artículo incluye tres regímenes diferentes.

En primer lugar, los bancos de datos personales de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia que fueron creados para fines administrativos; y aquellos sobre antecedentes personales que proporcionen dicho banco de datos a las autoridades judiciales o administrativas que lo requieran en virtud de disposiciones legales, quedan sujetos a las disposiciones legales de la ley 25.326, es decir, se rigen bajo el régimen común.

En segundo lugar, para los bancos de datos personales de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia creados con fines de defensa nacional o de seguridad pública, la ley no exige el consentimiento del afectado para el tratamiento de sus datos personales, a condición de que se cumplan los siguientes requisitos:

> a) se establezca a los fines de misiones legalmente asignadas para la defensa nacional, la seguridad pública o la represión de delitos.
>
> b) el tratamiento se limite a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de dichas misiones.
>
> c) los archivos sean específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

El art. 23 inc. 2 no adopta el principio de consentimiento para el tratamiento de datos personales, apartándose así de la regla general. A pesar de que en principio la solución parece razonable -ya que no sería lógico solicitar la autorización del titular cuando hay una investigación contra él- la redacción del inciso es demasiada general y permite a las autoridades estatales tratar datos personales más allá de lo que es estrictamente necesario y proporcional.

Por ejemplo, la legislación española –que fue utilizada como modelo para la redacción de la ley argentina- permite el tratamiento sin consentimiento pero

14 Cfr. Ley 25.326, Artículo 11.3.

establece que debe haber un "peligro real" para la seguridad pública[15]. La ley argentina no requiere la existencia de un "peligro real"[16].

En tercer lugar, el art. 23 inc.3 se refiere a los datos personales registrados con fines policiales. En este caso, el inciso sólo dispone que los mismos deban ser cancelados cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

La redacción de esta disposición presenta problemas debido a su indeterminación, imprecisión y amplitud. En primer lugar, el término "necesario" no permite que los titulares de los datos sepan con exactitud cuándo sus datos serán cancelados. En segundo lugar, deja a las autoridades con un gran margen de discrecionalidad para decidir cuándo o no cancelar los datos. Finalmente, no se establece la obligación de informar al titular que sus datos han ido cancelados, con lo cual el individuo puede permanecer en la incertidumbre de no saber si se ha cumplido la obligación de cancelación.

Mediante estas amplias excepciones establecidas, la ley 25.326 permite a los órganos estatales evadir en forma efectiva las prohibiciones de tratamiento y cesión de datos sin el consentimiento del titular o sólo cuando sea estrictamente necesario y proporcional al logro de un objetivo legítimo. Como consecuencia, los ciudadanos se ven privados de la principal herramienta para proteger sus datos.

Capacidad limitada de la autoridad de protección de datos

Las funciones de la Dirección Nacional de Protección de Datos Personales (DNPDP) establecidas por la ley y los decretos reglamentarios son extremadamente amplias y están diseñadas para un órgano independiente con autonomía financiera y con una estructura necesaria para realizar tales funciones de manera adecuada. Por nombrar algunas de las funciones: asesoramiento a los ciudadanos, regulación de poderes, control y registro de bases de datos públicas y privadas, y aplicación de sanciones en caso de incumplimiento, con amplia jurisdicción en todo el país.

De hecho, la versión inicial de la ley 25.326 intentó crear un órgano de control con "autonomía funcional" que actuaría "como un órgano descentralizado dentro de la estructura del Ministerio de Justicia y Derechos Humanos". Tal órgano tendría un director designado por el poder ejecutivo, con la aprobación del Senado, por un período de cuatro años. Sin embargo, estas garantías de autonomía funcional y autarquía financiera fueron dejadas de lado cuando el Poder Ejecutivo promulgó la ley parcialmente al dictar el decreto ejecutivo

15 El art. 22 inc. 2 de la LOPD dice: "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y cuerpos de Seguridad sin el consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.". Si bien el modelo para la elaboración de la ley argentina fue la derogada Ley Orgánica de Regulación del Tratamiento automatizado de los datos de carácter personal (LORTAD) el presente artículo es muy similar al anterior.

16 Cfr. Didier, Federico José "Protección de datos personales y tratamiento de datos con fines de seguridad en la legislación comparada" disponible en http://www.tecnoiuris.com.ar/publicaciones/proteccion-datos-personales1.php

995/00, que mantuvo al órgano dentro de la esfera del Poder Ejecutivo por razones financieras. Tal decisión fue clave para socavar la autonomía y efectividad de la DNPDP.[17]

Como ADC lo ha expuesto en su investigación publicada en Septiembre de 2014[18], la DNPDP ha visto negada las garantías de autonomía y autarquía financiera establecidas por la ley 25.326 y tiene que operar con un bajo presupuesto y un número limitado de personal para poder llevar a cabo actividades que exceden las reales capacidades institucionales disponibles. Como resultado de estas restricciones, la DNPDP no ha sido capaz de realizar plenamente sus funciones y en particular ha ejercido control limitado sobre el tratamiento y uso de datos personales por las autoridades estatales.

Destacamos como un signo positive que las nuevas autoridades de la DNPDP han mostrado un cambio de criterio en cuanto a medidas de control y cumplimiento, sin perjuicio de que las debilidades estructurales permanecen[19].

4. Registro e identificación de individuos: el uso de tecnología de biometría

Los riesgos a la privacidad y a la protección de datos personales que surgen de la pobre implementación de la legislación argentina sobre protección de datos personales son particularmente preocupantes en relación al creciente uso de tecnología de biometría.

El Registro Nacional de las Personas (ReNaPer) fue establecido por la ley en 1948[20]; en 1968, durante la dictadura militar, Argentina sancionó una ley que volvió obligatorio para todos los individuos la obtención de un documento de identidad[21].

En 2011, a través de un decreto del Poder Ejecutivo, el gobierno argentino estableció el Sistema Integrado de Identificación Biométrica (SIBIOS). Sibios integra la ya existente base de datos de documentos de identidad del Registro Nacional de las Personas (ReNaPer). Incluye las imágenes digital, huella dactilar, estado civil y el lugar de residencia de un individuo. El objetivo original de SIBIOS era facilitar la identificación de ciudadanos, permitiendo referencias cruzadas de datos para apoyar investigaciones criminales y como herramienta para funciones de seguridad preventiva. A ella pueden acceder la Dirección nacional de Inmigración, la Policía de Seguridad Aeroportuaria, la Gendarmería Nacional y otras dependencias gubernamentales, incluyendo entidades provinciales.

Existe un amplio rango de preocupaciones de derechos humanos relacionadas con Sibios.

17 Aun cuando el decreto reglamentario 1558/01, Artículo 29.1 sostiene que el "Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones"
18 https://adcdigital.org.ar/wp-content/uploads/2016/01/The-Collecting-State.pdf pag. 6
19 http://www.jus.gob.ar/datos-personales/la-direccion-en-los-medios/2016/04/27/la-direccion-de-proteccion-de-datos-personales-inicio-una-investigacion-sobre-uber.aspx
20 Ley N° 13,482, Creación del Registro Nacional de las Personas 29 de Septiembre, 1948.
21 Ley N° 17,671, Identificación, Registro y Clasificación del potencial humano nacional, 29 de Febrero, 1968.

En primer lugar, la pobre supervisión de los órganos de inteligencia y de seguridad, y el hecho de que un amplio número de instituciones gubernamentales pueden acceder a Sibios significa que el sistema podría facilitar la vigilancia masiva. Por cierto, el gobierno había dejado entrever la idea de que en el futuro esta tecnología será usada para buscar personas desaparecidas mediante un sistema CCTV integrado y que incluso más información personal –como el ADN y el escaneo del iris- puede ser incluida en esta base de datos.

En segundo lugar, el riesgo de que la base de datos de Sibios sea usada para fines distintos a aquellos originalmente previstos sin garantías adecuadas. Por ejemplo, Sibios fue utilizado para controlar los documentos de los votantes en las elecciones de Octubre de 2013[22] y de 2015[23]; el padrón electoral incorporó las fotos de los ciudadanos, aun cuando el consentimiento de los individuos no había sido obtenido para este uso.

Tal como el Relator Especial de la ONU sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo lo hizo notar en un informe dirigido al Consejo de Derechos Humanos, en principio, las leyes de protección de datos personales deben proteger a la información recolectada para un fin determinado de ser usada para otro.[24] Además, esta práctica falla en respetar el principio de que todo individuo debería ser capaz de saber qué autoridades públicas u órganos o individuos privados controlan o pueden controlar sus datos personales.[25]

La recolección, tratamiento y almacenamiento de fotografías de ciudadanos constituyen una amenaza evidente al derecho a la privacidad. Esto es particularmente así cuando los datos recolectados equivalen a datos personales sensibles, tales como (de acuerdo a la definición de la ley 25.326) datos que "puedan revelar raza, etnia o religión". Tales prácticas pueden generar perfiles personales que puedan potencialmente dar lugar a la creación de bases de datos con fines ilícitos y discriminatorios.

En tercer lugar, fueron identificadas debilidades en la seguridad de las bases de datos, poniendo a los datos personales en riesgo de acceso y usos ilegales por parte de terceros. A fines de 2013, luego de las elecciones de Octubre, un blogger identificó un código que luego fue utilizado por un programador para instalar un sitio que permitía que las imágenes sean recuperadas del registro electoral.[26] Sólo cuando esta falla tomó conocimiento público a través de los medios de comunicación, las fotografías fueron removidas, como pasó nuevamente en 2015.

El artículo 9 de la ley de protección de datos personales establece estándares para garantizar la seguridad y confidencialidad de los datos personales,

22 https://adcdigital.org.ar/wp-content/uploads/2016/01/Si-nos-conocemos-mas.pdf (page 17)
23 http://www.unosantafe.com.ar/pais/La-Camara-Electoral-levanto-las-fotos-de-ciudadanos-del-padron-20150716-0096.html
24 ONU doc. A/HRC/13/37, 28 de Diciembre de 2009.
25 Comité de Derechos Humanos Observación General N° 16 (1988) sobre el derecho al respeto a la privacidad, el hogar familiar y la correspondencia, y la protección del honor y la reputación (art. 17)
26 Ver Ignoring repeated warnings, Argentina biometrics database leaks personal data, 10 de Diciembre de 2013 disponible en: https://www.privacyinternational.org/node/342

incluyendo la prohibición de "registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad".

La Dirección Nacional de Protección de Datos Personales dictaminó medidas de seguridad obligatorias en la Directiva 11/2006[27], incluyendo niveles de seguridad básica, intermedia y crítica, de acuerdo a factores tales como la naturaleza del dato y los riesgos involucrados.

El gobierno falló en proteger los datos almacenados y no dio las respuestas adecuadas por los riesgos que implica el uso de tecnología de biometría y los sistemas de identificación digital.

Mediante sus fallas en la protección de datos personales, Argentina no está "asegurando que la información respecto a la vida privada de una persona no llegue a manos de personas que no están autorizadas por ley a recibir, procesar y usarla, y que nunca sea usada para fines incompatibles con el Pacto"[28].

27 DNPDP, Disposición 11/2006. Medidas de Seguridad par a el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y privacos", 19 de Septiembre de 2006

28 Comité de Derechos Humanos Observación General N° 16 (1988) sobre el derecho al respeto a la privacidad, el hogar familiar y la correspondencia, y la protección del honor y la reputación (art. 17)

5. Recomendaciones propuestas

En base a estas observaciones, la Asociación por los Derechos Civiles (ADC) y Privacy International proponen las siguientes recomendaciones al gobierno argentino:

- Tomar todas las medidas necesarias para asegurar que las actividades de vigilancia, tanto dentro como fuera de Argentina, se lleven a cabo de conformidad a las obligaciones contraídas bajo el Pacto, incluyendo el artículo 17: en particular, deberían tomarse medidas para asegurar que toda interferencia con el derecho a la privacidad se ajuste a los principios de legalidad, proporcionalidad y necesidad, sin que importe la nacionalidad o residencia de los individuos cuyas comunicaciones están bajo vigilancia; abstenerse de involucrarse en vigilancia masiva y regular en forma adecuada y transparente el intercambio de información con sus pares.

- Establecer directivas de supervisión fuertes e independientes con miras a prevenir abusos y asegurar que los individuos tengan acceso a remedies efectivos.

- Asegurar que la autoridad de protección de datos sea independiente y cuente con los recursos apropiados para cumplir sus funciones, incluyendo tener los poderes para investigar en forma efectiva violaciones a la protección de datos personales.

- Revisar el Sistema Integrado de Identificación Biométrica (SIBIOS) y limitar la recolección y el uso de datos personales para asegurar el cumplimiento con el derecho a la privacidad y los principios sobre protección de datos.