PRIVACY INTERNATIONAL

Informe de las partes interesadas
Examen Periódico Universal
26° período de sesiones - Argentina

El derecho a la privacidad en Argentina

Comunicación conjunta de la Asociación por los Derechos Civiles y Privacy International

Marzo 2017

Introducción

1. Este informe es presentado por la Asociación por los Derechos Civiles (ADC) y Privacy International (PI). La Asociación por los Derechos Civiles (ADC) es una organización no gubernamental, sin fines de lucro, ubicada en Buenos Aires, que promueve los derechos civiles y sociales en Argentina y otros países latinoamericanos. Fue fundada en 1995 con el objetivo de fortalecer una cultura jurídica e institucional que garantice los derechos fundamentales de la gente, basado en el respeto a la Constitución y los valores democráticos. PI es una organización de derechos humanos que trabaja en fomentar y promover el derecho a la privacidad y combatir la vigilancia alrededor del mundo[1].

2. ADC y PI desean manifestar algunas preocupaciones acerca de la protección y promoción del derecho a la privacidad, con el propósito de ser puestas a consideración en el próximo examen de Argentina, en la sesión 28 del Grupo de Trabajo del Examen Periódico Universal (EPU).

El derecho a la privacidad

3. La privacidad es un derecho fundamental, consagrado en numerosos tratados de derechos humanos. Es central en la protección de la dignidad humana y constituye la base de cualquier sociedad democrática. Además, la privacidad apoya y fortalece otros derechos, como la libertad de expresión, información, y asociación .

4. Las actividades que restringen el derecho a la privacidad, como la vigilancia y la censura, sólo se pueden justificar cuando son establecidas por ley, necesarias para lograr un objetivo legítimo, y proporcional al objetivo perseguido[3]. Como las innovaciones en las tecnologías de la información

1 Para mayor información, por favor remitirse a la investigación producida por ADC y PI, El Estado de la Privacidad, actualizado por última vez en Noviembre de 2016, disponible (en inglés) en https://www.privacyinternational.org/node/981

2 Declaración Universal de Derechos Humanos Artículo 12, Convención de las Naciones Unidas sobre Trabajadores Migrantes Artículo 14, Convención de Naciones Unidas sobre los Derechos del Niño Artículo 16, Pacto Internacional sobre Derechos Civiles y Políticos Artículo 17; convenciones regionales incluyendo artículo 10 de la Carta Africana sobre los Derechos y el Bienestar del Niño, Artículo 11 de la Convención Americana sobre Derechos Humanos, Artículo 4 de los Principios de la Unión Africana sobre Libertad de Expresión, Artículo de la Declaración Americana de los Derechos y Deberes del Hombre, Artículo 21 de la Carta Árabe sobre Derechos Humanos y Artículo 8 de la Convención Europea para la Protección de los Derechos Humanos y las Libertades Fundamentales; Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y Acceso a la Información, Principios de Camden sobre Libertad de Expresión e igualdad.

3 Declaración Universal de Derechos Humanos Artículo 29: Observación General Nº 27, adoptado por el Comité de Derechos Humanos de acuerdo al Artículo 4, inciso 4 del Pacto Internacional sobre Derechos Civiles y Políticos CCPR/C/21/Rev.1/Add.9, 2 de Noviembre de 2009; ver además Martin Scheinin “Informe del Relator especial sobre promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo” 2009, A/ HRC/17/34

han permitido formas de recopilación, almacenamiento e intercambio de datos personales previamente inimaginables, el derecho a la privacidad ha evolucionado hasta abarcar las obligaciones del Estado relacionadas con la protección de datos personales[4]. Varios instrumentos internacionales contienen principios de protección de datos[5] y muchas legislaturas han incorporado tales principios en leyes nacionales[6].

Seguimiento del EPU anterior

5. En el examen anterior de Argentina durante el segundo ciclo del EPU, no se hizo mención expresa del derecho a la privacidad en el informe presentado por Argentina, el informe del Grupo de Trabajo o las presentaciones de las partes interesadas.

Leyes internas sobre privacidad

6. Si bien la Constitución Argentina[7] no menciona la palabra "privacidad," sí se refiere a "acciones privadas" en su artículo 19, el cual ha sido interpretado por la Corte Suprema de Argentina como consagrando el derecho a la privacidad. El artículo dice "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe."

7. Además, el artículo 18 de la Constitución dice: "El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación."

8. Respecto a los datos personales, el Artículo 43 dice: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

4 Comité de Derechos Humanos, Observación General Nº 16 (1988) sobre el derecho al respeto a la privacidad, familia, domicilio y correspondencia, y protección del honor y la reputación (art. 17)

5 Ver Consejo de la Convención Europea para la Protección de Individuos con respecto al Procesamiento Automático de Datos Personales (Nº 108), 1981; Guía sobre protección de la privacidad y flujo transfronterizo de datos personales de la Organización para la Cooperación y el Desarrollo Económico (1980) y la Guía para la regulación de bases de datos personalizadas (Resolución 45/95 de la Asamblea General y E/CN.4/1990/72)

6 Hasta Diciembre de 2013, 101 países habían promulgado legislación sobre protección de datos personales.Ver: David Banisar National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (28 de Enero de 2014). Disponible en https://www.researchgate.net/profile/David_Banisar/publication/256011932_National_Comprehensive_Data_ProtectionPrivacy_Laws_and_Bills_2014_Map/links/569f88c008aee4d26ad26554/National-Comprehensive-Data-

7 Protection-Privacy-Laws-and-Bills-2014-Map.pdf
Disponible en
http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

Obligaciones Internacionales

9. Argentina ha ratificado varios tratados internacionales de derechos humanos que tienen implicaciones sobre la privacidad. Ha ratificado el Pacto Internacional de Derechos Civiles y Políticos, cuyo artículo 17 dispone que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación". El Comité de Derechos Humanos ha señalado que los Estados partes en el PIDCP tienen la obligación positiva de "adoptar medidas legislativas y de otra índole para dar efecto a la prohibición de tales interferencias y ataques, así como a la protección de este derecho [privacidad]."[8]

10. Desde el 14 de agosto de 1984, la Argentina es signataria de la Convención Americana sobre Derechos Humanos o "Pacto de San José de Costa Rica" (la "Convención Americana"), que en su artículo 11 establece que "nadie puede ser objeto de injerencia arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio, o en su correspondencia, ni de ataques ilegales a su honra o reputación."

11. A todos estos tratados ratificados por Argentina se les han concedido la misma jerarquía legal que la Constitución de acuerdo al Artículo 75.22[9].

AREAS DE PREOCUPACION

I. Vigilancia de las comunicaciones

12. La Ley de Inteligencia Nacional, Ley N° 25.520[10], regula la vigilancia de las comunicaciones llevadas a cabo por el Estado. La vigilancia de las comunicaciones privadas puede llevarse a cabo sólo si se emite una orden judicial específica para el caso en cuestión.

13. Hasta Diciembre de 2015, el único órgano estatal legalmente autorizado para llevar a cabo las vigilancias de las comunicaciones era el Departamento de Interceptación y Captación de las Comunicaciones (DICOM) bajo la órbita del Ministerio Público[11], pero a través del decreto N° 256/15 el Poder Ejecutivo transfirió el DICOM a la órbita de la Corte Suprema de Justicia de la Nación[12], que después reemplazó al DICOM por la Dirección de Captación de Comunicaciones (DCC)[13].

8 Observación General Nº 16 (1988), párrafo 1.
9 Ver http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm
10 Ver Ley Nº 25.520, Artículo 5. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm
11 Ley Nº 27.126, Artículo 17. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm
12 Decreto Nº 256/15. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257346/norma.htm
13 Centro de Información Judicial, La Corte Suprema creó la Dirección de Captación de Comunicaciones del Poder Judicial, 15 de Febrero de 2016. Disponible en http://cij.gov.ar/nota-19854-La-Corte-Suprema-cre--la-Direcci-n-de-Captaci-n-de-Comunicaciones-del-Poder-Judicial.html

14. La reforma del sistema de inteligencia en Argentina se vino gestando desde el escándalo que sacudió a las agencias de inteligencia en Diciembre de 2014, y se inició oficialmente a principios de 2015, cuando la entonces presidenta Cristina Fernández de Kirchner anunció planes para disolver la agencia de inteligencia[14]. Al momento de este anuncio, la ADC publicó un informe que acababa de realizar sobre el disfuncional y opaco sistema de inteligencia en Argentina. Las principales preocupaciones incluyeron la utilización del aparato de inteligencia del Estado en beneficio de la Presidencia, la falta de supervisión y transparencia, y la ausencia de rendición de cuentas de los presupuestos[15].

15. El anuncio de la reforma a principios de 2015 fue bien recibido por la sociedad civil a pesar de las preocupaciones por haberse iniciado el proceso a través de un decreto presidencial. Sin embargo, a principios de 2016, cuando se creó la nueva agencia - para reemplazar al DICOM -, se plantearon preocupaciones sobre ciertos aspectos de la recién creada DCC. Especialmente preocupante fue la estructura organizativa de la DCC, así como el muy corto plazo de duración del cargo de Director, de sólo un año. Este plazo no da suficiente tiempo para que el juez designado conozca cómo funciona el sistema, más si tenemos en cuenta que el conocimiento del sistema de interceptación de comunicaciones no es un requisito previo para la designación.También incluye una referencia muy amplia al uso de tecnologías de "minería de datos" para colaborar con los operadores legales a fin de obtener información de las bases de datos que se utilizarán en el proceso legal, sin más explicaciones[16].

16. A fines de septiembre de 2016, la Corte Suprema creó la Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado[17] para ayudar a las autoridades judiciales en casos de narcotráfico, trata de personas, secuestros, lavado de dinero, financiamiento del terrorismo y delitos contra el medio ambiente[18].

17. Dentro de la nueva Dirección, se creó la Oficina de Captación de Comunicaciones (OCC) para reemplazar a la DCC. La nueva posición institucional de la OCC - dentro de la Dirección- plantea ciertas inquietudes, ya que puede conducir a concebir la interceptación de las comunicaciones como un mero instrumento auxiliar para las investigaciones de crímenes.

18. Además del mandato otorgado previamente a la DCC, la recién creada Dirección de Asistencia Judicial en Delitos Complejos y Organizados ha ampliado las tareas de la OCC hasta incluir: desarrollar nuevas

14 BBC News, Argentina disolverá su agencia de inteligencia después de la muerte de un fiscal, 27 de Enero de 2015. Disponible en http://www.bbc.co.uk/news/world-latin-america-30995722

15 Asociación por los Derechos Civiles (2015) El (des) control democrático de los organismos de inteligencia en Argentina. Disponible en: http://www.adc.org.ar/wp-content/uploads/2015/01/2015-01-23-Informe-Final-Inteligencia.pdf

16 Asociación por los Derechos Civiles, Reflexiones sobre la creación de la Dirección de Captación de Comunicaciones, 19 de Febrero de 2016. Disponible en: https://adcdigital.org.ar/2016/02/19/reflexiones-sobre-la-creacion-de-la-direccion-de-captacion-decomunicaciones/

17 Acordada Corte Suprema: 30/2016. Disponible en: http://old.csjn.gov.ar/docus/documentos/verdoc.jsp?ID=100091

18 Artículo 4 de la Acordada de la Corte Suprema 30/2016

herramientas tecnológicas para mejorar la eficiencia de los procedimientos judiciales, facilitar a los jueces y fiscales el acceso a la información para detectar patrones comunes en los crímenes complejos y organizados y ofrecer nuevas herramientas para la interceptación de comunicaciones, entre otros.

Falta de supervisión integral e independiente de la vigilancia estatal

19. No hay una obligación de publicar informes sobre las actividades de vigilancia de las agencias de inteligencia. Sin embargo, de acuerdo al Artículo 12 de la ley de inteligencia nacional, Ley N°. 25.520, las agencias de inteligencia están obligadas a presentar informes anuales sobre sus actividades a la Comisión Bicameral Permanente de Fiscalización de los Organismos y Actividades de Inteligencia (en adelante Comisión)[19]. Debido a que estos informes son clasificados como confidenciales, no es posible averiguar si el sistema de supervisión está funcionando. Es más, los poderes del órgano de supervisión para obtener información relevante son muy limitados. Bajo el decreto reglamentario 950/2002[20] la Comisión tiene que obtener autorización de la Secretaría de Inteligencia, el mismo órgano sobre el cual la Comisión tiene la responsabilidad de controlar y cuya actividad tiene el mandato de supervisar.

20. Una investigación hecha por ADC reveló que el único informe que la Comisión tiene que enviar al Congreso y el Ejecutivo, tal como lo establece el Artículo 33.4 de la Ley, es el informe anual, y después de consultar con diversos diputados durante varios años, ADC descubrió que ellos nunca han recibido una copia de este informe[21].

21. Además, las agencias de inteligencia en Argentina operan con bastante autonomía y con poca supervisión efectiva. En los años recientes, se han visto cambios significativos en la organización de los servicios de inteligencia en Argentina.

22. Con el cambio de administración después de los elecciones presidenciales, en mayo de 2016, el decreto 656/16 dio aún más autonomía al director de la agencia de inteligencia, el cual puede aprobar su propia estructura organizacional, y emitir reglas complementarias y específicas. Esto puede conducir a la creación de una nueva estructura de la organización bajo secreto total, ya que el decreto no requiere que sea pública, lo que significa un revés importante en el proceso de la democratización del sistema de inteligencia[22].

19 Creada en 1991 por la Ley de Seguridad Interior Nº 24. 059
20 Artículo 11 y 20 del Decreto Reglamentario 950/2002
21 Asociación por los Derechos Civiles (2014). Quién vigila a los que vigilan. Estudio comparativo sobre sistemas de control de los organismos de inteligencia, pp. 12-13. Disponible en https://adcdigital.org.ar/wp-content/uploads/2016/01/Quien-Vigila-A-Quienes-Vigilan.pdf
22 A comienzos de 2016, el gobierno designó un nuevo Director y Subdirector de la Agencia Federal de Inteligencia (AFI). Gustavo Arribas y Silvia Majdalani, respectivamente. ADC, junto con otras organizaciones, plantearon inquietudes acerca de entrenamiento y experticia en asuntos de inteligencia de los funcionarios designados, lo cual pone en cuestión su idoneidad profesional para tan sensibles puestos.Savoia, Claudio. Ver. Clarín, 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; Asociación por los Derechos Civiles, ICCSI: Problemas en la designación de autoridades de la AFI, 30 March 2016. Disponible en: https://adcdigital.org.ar/2016/03/30/iccsiproblemas-designacion-autoridades-afi/

Capacidades de Vigilancia

23. Como resultado de la falta de transparencia de las políticas y prácticas de la vigilancia en Argentina, no es claro qué tipo de capacidades posee el país. Sin embargo, varios informes han aparecido en los últimos años dando cuenta de un sistema que difiere sustancialmente de lo que está indicado en la ley.

24. En julio de 2015, WikiLeaks publicó 400GB de material interno y correspondencia de una empresa italiana de vigilancia llamada Hacking Team[23]. Si bien no hay evidencia que Argentina compró equipo de Hacking Team, los documentos filtrados revelaron que el gobierno argentino se reunió con los representantes de Hacking Team, y la empresa presentó sus productos y servicios a varios órganos gubernamentales, incluyendo el Ministerio de Seguridad, la Dirección Nacional de Inteligencia Criminal, el Ministerio Público y la Unidad de Investigaciones Complejas[24]. Estamos preocupados de que estos órganos gubernamentales hayan tratado de comprar equipo de Hacking Team.

Registro obligatorio de la tarjeta SIM

25. La ley N°. 25.891 de 2004 sobre servicios de comunicaciones móviles exige el registro de todos los usuarios de teléfonos móviles[25]. En abril de 2016, la Ministra de Seguridad anunció que el Ministerio empezaría un trabajo en conjunto con el Ministerio de Comunicaciones para crear un registro nacional de las tarjetas SIM, con el fin de sacar del mercado a los teléfonos robados así como inutilizarlos con la ayuda de las empresas telefónicas[26].

26. El registro obligatorio de la tarjeta SIM viola la privacidad ya que limita la capacidad de los ciudadanos para comunicarse anónimamente. Además, facilita el rastreo y seguimiento de todos los usuarios por parte de las agencias de seguridad y las agencias de inteligencia. Investigaciones han demostrado que el registro de las tarjetas SIM no es una medida útil para combatir las actividades criminales, sino que en realidad alimenta el crecimiento de delitos relacionados con la identidad y de mercados negros para aquellos que desean permanecer en el anonimato[27].

23 Asociación por los Derechos Civiles, La ADC alerta: software de interceptación y vulneración a los derechos humanos, Agosto 2015. Disponible en: https://adcdigital.org.ar/wp-content/uploads/2015/08/Software-de-interceptacion-y-DDHH.-Informe-ADC.pdf

24 Ver documentación publicada por Wikileaks en Julio de 2015: https://wikileaks.org/hackingteam/emails/ emailid/587154; https://wikileaks.org/hackingteam/emails/emailid/765194; https://wikileaks.org/hackingteam/ emails/emailid/596983

25 Disponible http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

26 ENACOM, Resolution 2549/2016. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/261599/norma.htm; ENACOM, Se aprobó el procedimiento para el bloqueo de celulares robados, 20 de Mayo de 2016. Disponible en https://www.enacom.gob.ar/noticias/institucional/se-aprobo-elprocedimiento-para-el-bloqueo-de-celulares-robados_n1214; Telam, Fue detenida una banda que se dedicaba a clonar y comerciar de forma ilegal teléfonos celulares, 5 de Abril del 2016. Disponible en: http://www.telam.com.ar/notas/201604/142128-operativo-clonar-celulares-telefonos-patricia-bullrich.html

27 Donovan, K.P., y Martin, A.K., The rise of African SIM registration: Mobility, identity, surveillance and resistance, Information Systems and Innovation Group Working Paper No. 186, London School of Economics and Political Science, London.

27. Desde la resolución conjunta 6-E/2016[28] publicada en el Boletín Oficial del 10 de Noviembre de 2016, el Ministerio de Comunicaciones y el Ministerio de Seguridad resolvieron la creación del registro de identidad de los usuarios del servicio de comunicaciones móviles. La resolución forma parte de una acción gubernamental para combatir el crimen complejo y organizado, basado en el decreto 228/1629[29], que declara el estado de emergencia de la seguridad nacional.

28. La resolución establece que el Ente Nacional de Comunicaciones (ENACOM), tiene que adoptar las medidas necesarias "para identificar a todos los usuarios del Servicio de Comunicaciones Móviles del país en un Registro de Usuarios del Servicio de Comunicaciones Móviles." La responsabilidad de esta obligación recae en los operadores móviles, que tienen que proceder a la designación de las líneas telefónicas, es decir, relacionar cada número de teléfono con el nombre de su poseedor. Los operadores deben llevar a cabo el desarrollo - operación y administración del registro - a su propio costo y tienen que guardar la información de una manera "segura, auditable y durable," a disposición de una eventual solicitud del Poder Judicial o de la Fiscalía.

Reforma del Código Procesal Penal

29. En el 2016, Argentina inició un proceso de reforma de su Código Procesal Penal[30]. El proyecto de ley, presentado para consulta abierta, causó preocupación ya que propone el establecimiento de métodos especiales de investigación incluyendo: vigilancia remota de equipos informáticos, vigilancia mediante captura de imágenes y localización y seguimiento. Los impulsores de la ley argumentan que esas medidas de investigación están justificadas por la necesidad de reaccionar de manera apropiada y flexible para la difícil tarea de combatir la actividad criminal organizada y transnacional.

30. Si bien la presentación del proyecto indica que las medidas propuestas se pondrán en práctica una vez que se sometan a una prueba de razonabilidad y por un periódo de tiempo específico, respecto a los estándares recomendados de la ONU, el Consejo de Europa, la Corte Interamericana de Derechos Humanos, y el Tribunal Europeo de Derechos Humanos, algunas de sus disposiciones no cumplen con esos estándares mínimos. Las actividades que interfieren con el derecho a la privacidad y la libertad de expresión, como la vigilancia y la censura, solo se pueden justificar cuando son establecidas por la ley, necesarias para lograr un objetivo legítimo, y proporcional al objetivo perseguido.

28 Resolución conjunta del Ministerio de Comunicaciones y el Ministerio de Seguridad, 6-E/2016. Disponible en: https://www.boletinoficial.gob.ar/#!DetalleNorma/153684/20161110

29 Decreto 228/2016. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/258047/norma.htm

30 Angulo, M., Reforma al Código Procesal Penal: el Gobierno busca limitar las excarcelaciones, 6 de Octubre de 2016. Infobae. Disponible en: http://www.infobae.com/politica/2016/10/06/reforma-al-codigo-procesal-penal-elgobierno-busca-limitar-las-excarcelaciones/

31. En particular, quisimos expresar nuestras preocupaciones en cuanto a la introducción del "hackeo" como un método de investigación legal dentro de esta iniciativa, lo cual es particularmente preocupante. "Hackear" presenta un peligro único y grave a nuestra privacidad y seguridad. Por lo tanto, el punto de partida por defecto debería ser el cuestionamiento de si el hackeo puede ser un componente legítimo de la vigilancia del Estado.

32. Si el gobierno va a involucrarse en actividades de hackeo, sus facultades deberán ser establecidas por ley, ser necesarias para lograr un objetivo legítimo y proporcional al objetivo perseguido. Esta ley debe ser accesible al público y suficiente, clara y precisa para permitir a las personas prever su aplicación y la extensión de la intrusión. Debería estar sujeta a revisión periódica por medio de un proceso legislativo participativo. Los comentarios a la propuesta incluyen:

    a. Hay una omisión en brindar una definición de hackear y solo se refiere al uso de "software que permita o facilite el acceso remoto."

    b. Hay ausencia de información necesaria, en cuanto a quién va a ser la autoridad relevante para hacer este "acceso remoto" (el "hack").

33. El Relator Especial de la ONU sobre la libertad de expresión expresó sus preocupaciones sobre tal spyware ofensivo y dijo que "desde una perspectiva de derechos humanos, el uso de dichas tecnologías es muy preocupante. Troyanos, por ejemplo, no solo permiten a un Estado acceder a dispositivos, sino también les permite alterar - inadvertidamente o a propósito - la información contenida en el mismo. Eso amenaza el derecho a la privacidad y a la igualdad procesal con respecto al uso de tal evidencia en los procedimientos legales"[31].

Casos de vigilancia reportados

34. Aunque hay poca o ninguna información disponible respecto a las prácticas de vigilancia y las capacidades técnicas de las agencias de inteligencia, se han reportado varios casos de vigilancia.

35. Activistas de izquierda, sin embargo, todavía se sienten blanco por parte del gobierno. Hablando con Privacy International[32], Nicolás Tauber, abogado de derechos humanos, dijo que él se ha encontrado con varios casos de personas que han recibido mensajes de correo de voz que reproducían conversaciones telefónicas del pasado. Además, dijo que han habido múltiples ejemplos de abogados de derechos humanos que han sido víctimas de robo, en los cuales sólo los dispositivos electrónicos fueron robados. Él dijo que su propio estudio ha sido blanco y, que mientras los otros abogados -que no trabajan en derechos humanos- no habían sufrido ningún robo, su pen drive había desaparecido.

31 A/HRC/23/40, párrafo 62
32 Entrevista realizada en el transcurso del 2015.

36. Otro escándalo estalló a principios de 2015 cuando Alberto Nisman, un fiscal que había estado investigando la participación de Irán en el ataque contra la Asociación Mutual Israelita Argentina de Buenos Aires en 1994, fue encontrado muerto en su departamento el 18 de enero. Se presume que durante una investigación de 10 años, Nisman habría reunido grabaciones telefónicas que revelarían un acuerdo de impunidad entre los gobiernos de Irán y Argentina a cambio de beneficios económicos[33]. Nisman trabajaba estrechamente con Jaime Stiuso durante sus investigaciones, y se aduce que los servicios de inteligencia estarían involucrados en su muerte[34].

37. Especialmente preocupantes son los reportes de identificación de políticos, periodistas, y otros activistas. El 8 de diciembre de 2015, el Citizen Lab - de la Universidad de Toronto - publicó ""Packrat: Siete años de un actor amenazante de América del Sur", un informe de investigación que muestra una extensa campaña de malware, phishing y desinformación activa en varios países latinoamericanos, incluyendo Ecuador, Argentina, Venezuela, y Brasil[35]

.

38. El 20 de octubre de 2015, las ex diputadas Laura Alonso y Patricia Bullrich, presentaron una queja por presunto espionaje ilegal a periodistas, políticos, fiscales y jueces, llevado a cabo por la Agencia Federal de Inteligencia[36]. Junto con la queja, incluyeron una lista de más de 100 nombres de personas sujetas a vigilancia, incluyendo miembros de la Corte Suprema, varios jueces y fiscales federales, miembros de la oposición del gobierno de Kirchner y docenas de periodistas. La denuncia fue rechazada como falsa por el ex Ministro de Defensa, Agustín Rossi y el ex director de la AFI, Oscar Parrilli. Desde su revelación, no han habido nuevos desarrollos en cuanto al actual estado del caso y la investigación sobre la presunta interceptación de comunicaciones, incluyendo las realizadas desde Whatsapp, correo electrónico, teléfonos móviles, y computadoras personales.

39. El arresto del presunto narcotraficante colombiano Henry López Londoño en Argentina nos brinda una peculiar perspectiva sobre el uso de IMSI catchers para arrestar individuos, una práctica sobre la cual no hay mucho registro. El 27 de Abril de 2012, el juez argentino, Norberto Oyarbide autorizó a un equipo de la Policía colombiana a entrar en el país y rastrear a Londoño. Según la publicación argentina Diario Veloz, la policía colombiana solicitó permiso para usar el equipo que les permitiría localizar el teléfono de Londoño, pero indicó que el equipo no podría ser usado para escuchar o grabar conversaciones o mensajes en el teléfono. Es muy preocupante que Colombia pudiera solicitar autorización para rastrear el celular de Londoño sin aclarar específicamente qué tipo de equipo estaban planeando usar. Los IMSI catchers son rechazados a menudo como herramienta de vigilancia

33 Bracesco, G., Argentina, Iran and the strange death of Alberto Nisman, 20 de Febrero de 2015, Opinion, The Guardian. Disponible en: https://www.theguardian.com/commentisfree/2015/feb/20/argentina-iran-alberto-nisman-prosecutor-death

34 BBC News, Who killed Alberto Nisman?, Magazine, 28 de Mayo de 2015. Disponible en: http://www.bbc.co.uk/news/magazine-32887939

35 Scott-Railton, J., Marquis-Boire, M., Guarnieri, C., y Marschalek, M. (2015) Packrat: Seven Years of a South American Threat Actor, Citizen Lab, Diciembre 2015. Disponible en: https://citizenlab.org/2015/12/packrat-report/

36 La Nación, Denuncian espionaje de la Secretaría de Inteligencia a jueces, políticos y periodistas, 20 de Octubre de 2015. Disponible en: http://www.lanacion.com.ar/1838176-denuncian-espionaje-de-la-secretaria-deinteligencia-a-jueces-politicos-y-periodistas

localizada, cuando, en realidad, es equipamiento - como se dieron cuenta los servicios de inteligencia de Argentina - que podría usarse para vigilar indistintamente a cualquier persona y su entorno[37].

II. Régimen de protección de datos personales

40. Argentina tiene fuertes estándares de privacidad basados en la Constitución, así como leyes de protección de datos personales con estándares comparables a los 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.

41. Actualmente, la protección de datos personales en Argentina es regulada por la Ley N° 25326 que sigue estándares internacionales y se aplica al tratamiento de datos personales por organismos públicos y privados. Sin embargo, la ley no es aplicada en gran parte de sus disposiciones. Entre otras preocupaciones, el marco jurídico protector tiene dos debilidades estructurales: permisividad excesiva a favor del Estado en lo relativo al almacenamiento, procesamiento y transferencia de datos personales; y una agencia de control débil que depende del Poder Ejecutivo[38].

42. Reconociendo la necesidad de discutir una posible reforma de la ley N° 25326, el nuevo Director de Protección de Datos Personales de Argentina nombrado a principios de 2016 inició una consulta pública con todas las partes interesadas. ADC y PI han reconocido el proceso abierto, constructivo, y consultivo realizado por el Autoridad de Protección de Datos Personales y el Ministerio de Justicia de la República Argentina.

43. ADC y PI brindaron sus respectivos análisis acerca de sus evaluaciones de la ley propuesta. Si bien damos la bienvenida a la planeada reforma de la Autoridad de Protección de Datos para asegurar que tenga la independencia y autonomía en cuanto a su mandato, función, y operaciones, seguimos preocupados por varias disposiciones de la ley propuesta. Estas incluyen:

    a. La necesidad de redefinir lo que constituyen datos accesibles al público, a los cuales se les aplican menos protecciones legales (artículo 2).

    b. La introducción del consentimiento tácito sin condiciones y guías claras acerca de los contextos en los que el consentimiento tácito será suficiente (Artículo 12)

    c. La inclusión de los datos genéticos y biométricos como datos

37 Blum-Dumontet, E., IMSI Catch 22: Understanding the Role of Spying Equipment in the Mi Sangre Case, 1 de Marzo de 2017, Privacy International. Disponible en: https://medium.com/@privacyint/imsi-catch-22-understanding-therole-of-spying-equipment-in-the-mi-sangre-case-23c27a001f7c

38 Ver: Presentación conjunta de la Asociación por los Derechos Civiles y Privacy International antes de la consideración de Argentina, Comité de Derechos Humanos, 117º sesión. Disponible en: https://www.privacyinternational.org/sites/default/files/argentina_english.pdf

sensibles para concederles el nivel más alto de protección (artículos 2 y 16);

d. La potencial interpretación amplia de las excepciones 1-3 del artículo 36, y que permitiría a cualquier autoridad responsable del tratamiento de una base de datos pública no tener que cumplir con ninguno de los derechos de los interesados, previstos en el capítulo III ni con ninguna de las salvaguardias previstas en el capítulo II.

e. A las agencias del estado se les permite evitar la prohibiciones de procesar o transferir los datos sin el consentimiento del dueño o solo cuando sea estrictamente necesario y proporcional al logro de un objetivo legítimo. Como consecuencia, los ciudadanos están privados de la principal herramienta para proteger la privacidad de sus datos (artículo 58).

44. Es extremadamente importante que Argentina tome las medidas necesarias para asegurar que su régimen de protección de datos personales cumpla los estándares más altos y respete sus obligaciones domésticas e internacionales, dado algunos preocupantes incidentes de violación de datos ocurridos en los últimos años y el despliegue cada vez mayor de sistemas de gobernanza basados en datos.

45. Datos electorales: a finales de 2014, tras las elecciones de octubre, un blogger identificó un código que estaba siendo usado por un programador para construir un sitio que permitía que las imágenes sean recuperadas del padrón electoral[39]. Después de que la noticia concitó la atención pública a través de los medios de comunicación, las fotografías fueron retiradas. En Julio de 2016, el Jefe de Gabinete emitió la Resolución 166/2016[40] mediante la cual la Administración Nacional de Seguridad Social (ANSES) compartirá la base de datos (que contiene datos como nombre, número de documento de identidad, domicilio, número de teléfono, dirección de correo electrónico, fecha de nacimiento y estado civil) con la Secretaría de Comunicación Pública, que depende funcionalmente del Jefe de Gabinete, para mejorar la estrategia de comunicaciones del gobierno. La decisión fue cuestionada por expertos en protección de datos personales[41] y miembros de la oposición[42], que alegaron que la transferencia de datos no se ajusta al principio de finalidad, porque los datos estaban siendo recolectados para la administración eficiente del sistema de seguridad social, no para actividades de comunicaciones o relaciones públicas.

39 Pirlot de Corbion, A., Ignoring repeated warnings, Argentina biometrics database leaks personal data, 9 de Diciembre de 2013. Privacy International. Disponible en: https://www.privacyinternational.org/node/342

40 Disponible en: https://www.boletinoficial.gob.ar/pdf/linkQR/TFNSL3lFWGNOOUErdTVReEh2ZkU0dz09

41 Ver: http://www.ditc.com.ar/2016/07/29/sobre-el-acuerdo-anses-una-interpretacion-de-la-25-326-distinta-a-lautilizada/

42 Política Argentina, Sectores de la oposición cuestionan la utilización de bases de datos de la Anses, 26 de Julio de 2016. Disponible en: http://www.politicargentina.com/notas/201607/15546-sectores-de-la-oposicioncuestionan-la-utilizacion-de-bases-de-datos-de-la-anses.html

46. SIBIOS: En 2014, el RENAPER emitió la resolución 3020/14[43] en la que se estableció que el único documento de identificación válido es la nueva tarjeta digital, y que los datos biométricos de los ciudadanos serán digitalizados y recogidos en una base de datos unificada. Desde Noviembre de 2009, el RENAPER ha emitido más de 41 millones de tarjetas nuevas. La base de datos en cuestión es el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) creado en 2011 por el Decreto 1766/11[44] bajo la órbita del Ministerio de Seguridad. Los datos biométricos recolectados por SIBIOS consisten principalmente de huellas dactilares y patrones faciales. Los principales usuarios de SIBIOS son la Policía Federal, la Gendarmería Nacional, la Prefectura Naval, la Policía de Seguridad Aeroportuaria, el Registro Nacional de las Personas y la Dirección Nacional de Inmigración; además, cada provincia puede firmar un acuerdo de adhesión para incluir a su Policía como usuaria y como proveedora de datos. Las preocupaciones principales expresadas anteriormente incluyen la ausencia de la necesidad de obtener el consentimiento del titular de los datos cuando los datos son tratados para los funciones del Estado o para el cumplimiento de obligaciones jurídicas, la ausencia de orden judicial como un prerrequisito para acceder y obtener la información de ciudadanos del Sistema, así como amenazas de seguridad sobre bases de datos unificadas.

47. El sistema de transporte público: El 4 de febrero de 2009, por decreto 84/09[45], el Poder Ejecutivo lanzó una nueva tarjeta de transporte, la tarjeta SUBE (Sistema Único de Boleto Electrónico), bajo la supervisión de la Secretaría de Transporte dentro del Ministerio de Planificación. Aunque uno puede comprar la tarjeta SUBE sin documentos de identidad en kioscos en las varias ciudades donde se implementa el sistema, el usuario tiene que registrar la tarjeta y vincularlo a sus datos personales como nombre, apellido, tarjeta de identificación, género, fecha de nacimiento, correo electrónico y número de teléfono para consultar el saldo de la tarjeta o los viajes, o para acceder a las tarifas sociales disponibles a grupos como jubilados. Existen reportes de que la base de datos es vulnerable y accesos sin autorización has sido demostrados por un grupo llamado Anons.ar, miembros de Anonymous. El registro de las transacciones fue publicado en línea por el grupo[46].

43 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/237457/norma.htm
44 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm
45 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/150000-154999/150105/texact.htm
46 La Nación, Exponen en la Red los registros de viajes de la tarjeta SUBE, 30 de Enero de 2012. Disponible en: http://www.lanacion.com.ar/1444623-exponen-en-la-red-los-registros-de-viajes-de-la-tarjeta-sube

Recomendaciones

48. Nosotros recomendamos que el gobierno de Argentina:

1. Instrumente todas las medidas necesarias para asegurar que sus actividades de vigilancia, tanto dentro como fuera de Argentina, se ajusten a sus obligaciones de acuerdo al Pacto, incluyendo el artículo 17; en particular, deben adoptarse medidas para asegurar que cualquier interferencia con el derecho a la privacidad cumpla con los principios de legalidad, proporcionalidad y necesidad, independientemente de la nacionalidad o la ubicación de los individuos cuyas comunicaciones están bajo vigilancia; abstenerse de participar en la vigilancia masiva y regular de manera adecuada y transparente el intercambio de información con sus socios.

2. Establezca mecanismos de vigilancia fuertes e independientes del mandato y las funciones de la agencia de inteligencia, y la recién establecida Oficina de Captación de Comunicaciones, con un enfoque en prevenir abusos y asegurar que los individuos tengan acceso a remedios efectivos.

3. Asegure que cualquier reforma del Código Procesal Penal cumpla con las obligaciones nacionales e internacionales de derechos humanos de la Argentina y en particular en cuanto al derecho a la privacidad.

4. Derogue la disposición de la Ley N° 25.891 que impone la retención obligatoria de los datos de comunicación y el registro de la tarjeta SIM.

5. Asegurar que cualquier reforma de la Ley. N° 25326 aborde las principales deficiencias del actual marco jurídico para garantizar el respeto y el cumplimiento de los principios de protección de datos internacionalmente reconocidos.

6. Revise las iniciativas basadas en datos, incluyendo el padrón electoral, el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) y la tarjeta SUBE, y limite la recolección y el uso de datos personales para asegurar el respeto al derecho a la privacidad y a los principios de protección de datos personales.

La versión española de este informe fue traducida por Sarah Goodman con el apoyo de Eduardo Ferreyra.