



# Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina

Por Verónica Ferrari y Daniela Schnidrig  
*con la colaboración de la Electronic Frontier Foundation*

Diciembre de 2015



*Verónica Ferrari y Daniela Schnidrig, investigadoras de la Iniciativa por la Libertad de Expresión en Internet del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE). El informe fue elaborado con los aportes y supervisión de Eduardo Bertoni, Centro de Estudios en Libertad de Expresión y Acceso a la Información.*

Agradecemos la contribución de Katitza Rodríguez, International Rights Director por la revisión sustantiva del informe, Kim Carlson y David Bogado por la corrección de estilo y traducción.

El presente informe forma parte del proyecto regional “Vigilancia y Derechos Humanos” llevado a cabo en ocho países de América Latina por la Electronic Frontier Foundation (EFF), una organización internacional sin fines de lucro que desde 1990 defiende la libertad de expresión y la privacidad en el entorno digital.

El Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo (UP) tiene como objetivo producir, desde una perspectiva académica, investigaciones que se constituyan en herramientas útiles para los distintos sectores involucrados en la defensa y promoción de los derechos de libertad de expresión y acceso a la información. Dentro del CELE, funciona la Iniciativa por la Libertad de Expresión en Internet (iLEI), un programa especial dedicado a promover mejores políticas en materia de internet.



“Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina” por el Centro de Estudios en Libertad de Expresión y Acceso a la Información y la Electronic Frontier Foundation está disponible bajo Licencia Creative Commons Reconocimiento 4.0 Licencia Internacional.

## Índice de contenido

|   |    |
|---|----|
| 1. Fuerza Normativa de Tratados Internacionales de Derechos Humanos que Puedan Afectar la Vigilancia de las Comunicaciones..... | 4  |
| 1.1 ¿Cómo Recoge el Estado la Obligación de Cooperación Internacional en Materia de Intercambio de Información?.....            | 4  |
| 1.2 ¿Tiene Tratados Internacionales que Incluyen la Doble Incriminación como Condicionante para Cooperar?.....                  | 5  |
| 2. Marco Constitucional.....  | 6  |
| 3. Marco Legal.....   | 8  |
| 3.1 La Vigilancia de las Comunicaciones en el Contexto Penal.....   | 8  |
| 3.2 Delitos Electrónicos y Otras Sanciones.....   | 8  |
| 3.3 Vigilancia de las Comunicaciones de las Actividades de Inteligencia y Contrainteligencia.....                               | 10 |
| 3.4 Vigilancia de las Comunicaciones en la Normativa de Telecomunicaciones.....   | 14 |
| 3.5 Normativa sobre Retención de Datos.....   | 15 |
| 3.6 Reglas para el Allanamiento del Domicilio y Registro y Secuestro de Equipos Informáticos.....                               | 16 |
| 3.7 Otras normativas.....   | 18 |
| 4. Jurisprudencia.....  | 26 |
| 5. Marco Institucional.....   | 28 |
| 5.1 Organigrama de los Órganos Involucrados en la Persecución Penal.....  | 28 |
| 5.2 Diagrama de Proceso Penal Para Interceptar una Comunicación.....  | 29 |
| 5.3 Organigrama de los Órganos Inteligencia.....  | 30 |
| 5.4 Proceso de los Cuerpos de Inteligencia para Interceptar Comunicaciones.....   | 31 |
| 6. Formas de Control.....   | 34 |
| 6.1 Entidades Autorizadas Para Intervenir Una Comunicación Privada Sin Orden Judicial.....                                      | 34 |
| 6.2 Obligación de Reportes de Transparencia y Supervisión Pública.....  | 34 |
| 6.3 Mecanismos de Notificación Diferida.....  | 35 |
| 7. Aplicación de la Ley y Diseños Institucionales.....  | 36 |
| 7.1 Causa por Escuchas Ilegales en la Ciudad de Buenos Aires.....   | 36 |
| 7.2 Proyecto X.....   | 36 |
| 7.3 Compra de Equipamiento para Vigilancia de las Comunicaciones.....   | 37 |
| 7.4 La Muerte del Fiscal Nisman y la Reforma al Sistema de Inteligencia.....  | 38 |
| 8. ¿Respeto Argentina los Estándares Internacionales de Derechos Humanos Frente a la Vigilancia Estatal?.....                   | 39 |
| 9. Recomendaciones.....   | 51 |
| Notas Finales.....  | 53 |

# 1.

## **Fuerza Normativa de Tratados Internacionales de Derechos Humanos que Puedan Afectar la Vigilancia de las Comunicaciones**

### **1.1 ¿Cómo Recoge el Estado la Obligación de Cooperación Internacional en Materia de Intercambio de Información?**

Son numerosos los tratados internacionales que contienen previsiones sobre derechos que pueden ser afectados por la vigilancia de las comunicaciones. El primer derecho asociado con la vigilancia es el derecho a la privacidad y a la intimidad, contemplado por distintos instrumentos internacionales.

Por ejemplo, la Convención Americana sobre Derechos Humanos—en adelante, CADH—prevé en su artículo 11 que “Nadie puede ser objeto de injerencias 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”. La Declaración Universal de Derechos Humanos—en adelante, DUDH—contempla una redacción muy similar en su artículo 12, al igual que el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, que establece lo mismo y agrega que “Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

Los tratados de derechos humanos ratificados por la Argentina son plenamente vinculantes y aplicables en el derecho interno. La Corte Suprema de Justicia de la Nación dejó esto en claro en el fallo “Ekmekdjian c. Sofovich”, un caso sobre libertad de expresión y derecho a réplica del año 1992. Al respecto, la Corte sostuvo que la Convención de Viena—en vigor en Argentina desde 1980—le confiere primacía a las convenciones de derecho internacional por sobre el derecho interno y que, además, “cuando la Nación ratifica un tratado que firmó con otro Estado, se obliga internacionalmente a que sus órganos administrativos y jurisdiccionales lo apliquen a los supuestos que ese tratado contemple, siempre que contenga descripciones lo suficientemente concretas de tales supuestos de hecho que hagan posible su aplicación inmediata.”<sup>1</sup>

En 1994, durante la última reforma a la Constitución Nacional argentina, esta doctrina fue expresamente adoptada al establecer la jerarquía constitucional de los tratados internacionales de derechos humanos ratificados por el país.<sup>2</sup>

Esto no deja lugar a dudas que las protecciones a la posible afectación de derechos humanos en casos de vigilancia de las comunicaciones por el Estado, contempladas en tratados de derechos humanos ratificados por Argentina, son plenamente operativos y deben ser respetados por el Estado.

## 1.2 ¿Tiene Tratados Internacionales que Incluyen la Doble Incriminación como Condicionante para Cooperar?

Respecto del requisito de la doble incriminación (*dual criminality*) como condicionante para la cooperación jurídica internacional en materia penal, deben analizarse los distintos tratados celebrados con otros países.

Argentina cuenta con la Ley No. 24.767 de Cooperación Internacional en Materia Penal, que regirá para casos con Estados con los que no se haya celebrado un tratado de cooperación, o para cuestiones que no estén incluidas en dichos tratados. Esta ley dispone que, para que proceda la extradición de una persona, el hecho material del proceso deberá constituir un delito en la ley argentina y la ley del Estado requirente, y que tenga prevista una pena privativa de libertad con mínimo y máximo tales que su semisuma sea al menos de un año.<sup>3</sup>

Para los casos en los que exista un tratado de asistencia o de cooperación internacional, deberá respetarse lo que éste establezca. Algunos instrumentos de cooperación contienen el requisito de doble incriminación, como por ejemplo el Tratado de Extradición entre la República Argentina y la República Oriental del Uruguay,<sup>4</sup> que establece que los delitos que dan lugar a la extradición son aquellos “tipificados como delito por las leyes de ambas Partes, cualquiera sea la denominación de dicho delito, que sean punibles con una pena privativa de libertad cuya duración máxima no sea inferior a dos años.”<sup>5</sup>

En cambio, el Convenio entre la República Argentina y la República del Salvador sobre Asistencia Jurídica en Materia Penal,<sup>6</sup> por ejemplo, establece que “La asistencia se prestará aun cuando el hecho por el cual se procede en, la Parte requirente no sea considerado como delito por la legislación de la Parte requerida”.

En definitiva, habrá que analizar cada tratado de cooperación en particular, pero es positivo que el requisito de doble incriminación esté incluido en la Ley de Cooperación Internacional.

## 2.

### Marco Constitucional

El marco jurídico constitucional argentino protege derechos fundamentales que pueden ser afectados por la vigilancia de las comunicaciones.<sup>7</sup> Como comentamos en la sección anterior, los tratados internacionales de derechos humanos ratificados por el país tienen jerarquía constitucional, por lo tanto todas las protecciones a derechos relacionados con la vigilancia que éstos contengan son plenamente exigibles en nuestro régimen jurídico.

Además de la protección del derecho internacional, la Constitución Nacional contempla la protección de distintos derechos relacionados que podrían ser afectados por la vigilancia de las comunicaciones. Respecto del derecho a la intimidad y a la privacidad, la Constitución Nacional sostiene que “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”.<sup>8</sup>

La Constitución establece, también, la inviolabilidad del domicilio y de las comunicaciones, en tanto “...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...”.<sup>9</sup> Si bien menciona a la correspondencia epistolar, la Corte Suprema ha ampliado esta protección, entendiendo que las comunicaciones a través de Internet también están protegidas por esta cláusula constitucional.<sup>10</sup> (Ver sección “Jurisprudencia”).

Por último, la figura del habeas data también está contemplada en la Constitución. Ésta dispone que “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.”<sup>11</sup>

La Constitución prevé, además, la acción de amparo. Ésta es una acción expedita y rápida, que podrá interponerse “siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.”<sup>12</sup> Ésta

fue la herramienta legal que utilizó Halabi, un abogado que solicitó a la Corte Suprema que declara la inconstitucionalidad de un artículo sobre retención obligatoria de datos porque era violatorio de la intimidad y además violaba el secreto profesional. Sobre este caso nos explayaremos en la sección “Jurisprudencia”.

Podemos concluir que el marco constitucional argentino contempla una fuerte protección a los derechos a la intimidad, privacidad, protección de datos personales e inviolabilidad de las comunicaciones. A continuación, analizaremos el marco más amplio de las leyes y normativa que regulan esta protección de forma específica.

## 3.

### Marco Legal

#### 3.1 La Vigilancia de las Comunicaciones en el Contexto Penal

La legislación penal argentina contiene varias disposiciones respecto de la interceptación de comunicaciones privadas. Por un lado, se criminaliza la interceptación de comunicaciones privadas por parte de terceros. Por otro lado, se regulan las condiciones en las que el Estado puede interferir comunicaciones en el marco de un proceso penal.

En cuanto a las condiciones en las que el Estado puede interferir comunicaciones en el marco de un proceso penal, encontramos algunas disposiciones en el nuevo Código Procesal Penal Nacional, recientemente aprobado<sup>13</sup>. Éste establece, en su sección de principios y garantías procesales, el deber de respetar la protección de la intimidad y la privacidad, abarcando las comunicaciones. Este nuevo cuerpo sostiene que:

Se debe respetar el derecho a la intimidad y a la privacidad del imputado y de cualquier otra persona, en especial la libertad de conciencia, el domicilio, la correspondencia, los papeles privados y las comunicaciones de toda índole. Sólo con autorización del juez y de conformidad con las disposiciones de este Código podrán afectarse estos derechos.<sup>14</sup>

En la sección correspondiente ampliaremos sobre el procedimiento penal para ordenar la interceptación de una comunicación.

#### 3.2 Delitos Electrónicos y Otras Sanciones

En cuanto a la criminalización de la interceptación de comunicaciones, el Código Penal contempla las siguientes penas para la violación de la privacidad:

Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o capture comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.<sup>15</sup>

Se pena además, a quien a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido, con una pena agravada si se trata de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.<sup>16</sup>

El Código Penal contempla penas también contra quienes hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros, con la excepción de quienes hubieran obrado con “el propósito inequívoco de proteger un interés público.”<sup>17</sup>

Por último, se pena a quien “a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley; ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales”, agravando la pena si se trata de un funcionario público.<sup>18</sup>

La Ley No. 25.520 de Inteligencia Nacional, que analizaremos más en detalle en la sección siguiente, incorporó en 2015 ciertas disposiciones penales para castigar a quien, participando en forma permanente o transitoria de las tareas reguladas en dicha ley, “indebidamente interceptare, capture o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos.”<sup>19</sup>

Esta ley también tipifica el delito de quien, con orden judicial y estando obligado a hacerlo, “omitiera destruir o borrar los soportes de las grabaciones, las copias de las intervenciones postales, cablegráficas, de facsímil o de cualquier otro elemento que permita acreditar el resultado de las interceptaciones, captaciones o desviaciones.”<sup>20</sup> Siguiendo lo que establece esta normativa, se castiga también a todo funcionario o empleado público que realice acciones de inteligencia prohibidas por las leyes.<sup>21</sup>

### **3.3 Vigilancia de las Comunicaciones de las Actividades de Inteligencia y Contrainteligencia**

El marco regulatorio de las actividades de inteligencia está dado en Argentina, en primer término, por la Ley 25.520 de Inteligencia Nacional de 2001<sup>22</sup> y por la recientemente aprobada ley 27.126 que la modifica en muchos de sus aspectos más sustanciales.<sup>23</sup> Forman parte de este marco normativo, asimismo, los decretos que promulgan<sup>24</sup> y reglamentan<sup>25</sup> ambas leyes y por un decreto reciente que establece la denominada Nueva Doctrina de Inteligencia Nacional.<sup>26</sup>

La ley 27.126 aprobada este año modifica aspectos de la normativa y, fundamentalmente, disuelve el organismo encargado de las actividades de inteligencia y lo reemplaza por la Agencia Federal de Inteligencia (AFI).

Según este marco regulatorio, los organismos de inteligencia deberán desarrollar sus actividades en línea con lo que establecen la Constitución Nacional y los tratados de derechos humanos suscriptos por la Argentina, analizados anteriormente.<sup>27</sup>

Según este cuerpo normativo la “inteligencia nacional” en Argentina se define como la actividad que consiste en la “obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación.”<sup>28</sup>

Este marco legislativo vinculado a la inteligencia nacional, tal como señala la Asociación por los Derechos Civiles (ADC) en un trabajo reciente sobre esta temática, debe leerse en conjunto con las leyes de Defensa Nacional<sup>29</sup> y de Seguridad Interior.<sup>30</sup> ADC, en su informe, señala que este grupo de normas “busca delimitar actividades y establecer prohibiciones taxativas con el objetivo explícito de impedir abusos” y agrega que uno de sus objetivos principales es el de distinguir los conceptos y actividades vinculados, por un lado, a la defensa nacional y, por otro, a la seguridad nacional.<sup>31</sup>

Por un lado, la ley de Defensa Nacional regula lo vinculado a las actividades de inteligencia militar que apuntan a enfrentar las “agresiones externas”. La ley es clara al señalar que, en

ningún caso, se incluirá cuestiones vinculadas a la política interna dentro de estas actividades.<sup>32</sup>

Por su parte, la ley de Seguridad Interior excluye a las fuerzas armadas de las tareas de seguridad interior. Se exceptúan situaciones en las que el Poder Ejecutivo considere que no puede afrontar determinada amenaza con fuerzas de seguridad interna como la Policía Federal, las policías provinciales, la Gendarmería Nacional, etcétera. Esta ley regula, asimismo, lo que tiene que ver con las actividades de inteligencias llevadas a cabo por las fuerzas de seguridad y policiales.<sup>33</sup>

Como señalamos antes, el marco regulatorio actual señala que el funcionamiento del sistema de inteligencia en Argentina deberá ajustarse estrictamente a las previsiones que aparecen en la Constitución Nacional y en las normas legales y reglamentarias vigentes.<sup>34</sup> Y establece que ningún organismo de inteligencia argentino podrá:

Realizar tareas represivas, poseer facultades compulsivas, cumplir, por sí, funciones policiales. Tampoco podrán cumplir funciones de investigación criminal, salvo ante requerimiento específico y fundado realizado por autoridad judicial competente en el marco de una causa concreta sometida a su jurisdicción,<sup>35</sup> o que se encuentre, para ello, autorizado por ley, en cuyo caso le serán aplicables las reglas procesales correspondientes.<sup>36</sup>

A partir de la modificación que trajo la ley 27.126, el marco legislativo establece que son las autoridades máximas de cada organismo del sistema de inteligencia las que ordenan estas actividades. De todas formas, señala que “en caso de urgencia” estas actividades podrán iniciarse, debiendo ser informadas de manera inmediata a esas máximas autoridades.<sup>37</sup>

Específicamente, en cuanto a la interceptación y captación de comunicaciones privadas, el marco legislativo argentino en materia de inteligencia establece que solo se podrán solicitar mediante una autorización judicial.<sup>38</sup> La ley agrega que esta autorización, “deberá formularse por escrito y estar fundada indicando con precisión el o los números telefónicos o direcciones electrónicas o de cualquier otro medio, cuyas comunicaciones se pretenda interceptar o captar.”<sup>39</sup>

Si bien esta cuestión será analizada más en detalle en otro apartado, vale la pena señalar que, a partir de la reciente reforma del sistema de inteligencia nacional en el 2015, se transfiere la Dirección de Observaciones Judiciales, el único órgano del Estado argentino que puede llevar adelante las interceptaciones o captaciones de las comunicaciones—siempre que sean autorizadas u ordenadas por la autoridad judicial competente, como señalamos antes—al ámbito de la Procuración General de la Nación del Ministerio Público, un “órgano independiente con autonomía funcional y autarquía financiera.”<sup>40</sup>

Este marco regulatorio señala que los organismos de inteligencia deben enmarcar sus actividades “inexcusablemente” dentro de lo que establece la Ley de Protección de Datos Personales,<sup>41</sup> que analizaremos más adelante.

La revelación o divulgación de información adquirida por los organismos de inteligencia con motivo del ejercicio de sus funciones, requerirá sin excepción de una orden o dispensa judicial, como se comentó en apartados anteriores.<sup>42</sup>

La ley de Inteligencia Nacional hace también referencia a los bancos de datos almacenados por los órganos que componen el sistema de inteligencia argentino. Según la ley, estos organismos deberán tenerlos centralizados en el denominado Banco de Protección de Datos y Archivos de Inteligencia, que estará a cargo de un funcionario que deberá velar por las “las condiciones y procedimientos respecto a la recolección, almacenamiento, producción y difusión de la información obtenida, mediante tareas de inteligencia.”<sup>43</sup>

La regulación establece, también, que cada uno de estos bancos de protección de datos tendrá que controlar el ingreso y la salida de información garantizando su reserva constitucional y legal; que los datos recabados por las actividades de inteligencia que no sirvan para los fines establecidos por el marco que regula esta actividad, serán destruidos; y garantizar que no se almacene información por motivos de raza, creencias religiosas, acciones privadas, actividades políticas, pertenencia a organizaciones sociales, entre otras.<sup>44</sup>

Como se explicó anteriormente, la ley establece sanciones penales para aquellos integrantes de los servicios de inteligencia que indebidamente intercepten, capten o desvíen comunicaciones que no le estuvieran dirigidas.<sup>45</sup>

### **3.3.1 Nueva Doctrina de Inteligencia Nacional**

En el marco de este proceso de reforma del sistema de inteligencia en Argentina al que hicimos mención en secciones anteriores, recientemente en el 2015, se aprobó la denominada “Nueva Doctrina de Inteligencia Nacional para el proceso de reforma y modernización del Sistema de Inteligencia”<sup>46</sup> que, gran medida, apunta a definir los nuevos objetivos y tareas de la recientemente creada AFI.

Según el decreto que la crea, esta nueva doctrina apunta a una reforma y modernización del Sistema de Inteligencia Nacional.<sup>47</sup> Incluye una visión integral del concepto de inteligencia definida como “recolección, gestión y análisis de la información”<sup>48</sup> y entendido como una “actividad institucional que se inscribe dentro del marco del Estado constitucional social y democrático de derecho y que apunta a dar cuenta de los desafíos, coacciones y conflictos que ponen en riesgo la defensa y la seguridad democráticas del pueblo argentino.”<sup>49</sup>

El primero de los anexos que acompaña el decreto que fija este cuerpo doctrinario, señala que las actividades de inteligencia en Argentina “se inscriben en la esfera específica del sistema democrático de defensa nacional y de seguridad interior y constituyen acciones fundamentales para la estabilidad y protección del sistema democrático.”<sup>50</sup>

Y, señala, específicamente, que la inteligencia nacional debe velar por la protección y el cuidado de los argentinos, y no “espíarlos” (*las comillas están en el original*). Por ello, define al sistema de inteligencia nacional en tanto un observatorio que se dedicará, exclusivamente, a “la producción y gestión de conocimientos acerca del conjunto de problemáticas relevantes en materia de defensa nacional y seguridad interior.”<sup>51</sup>

Esta nueva doctrina define a la seguridad interior como la que comprende “los fenómenos delictivos violatorios de las libertades y derechos de las personas y del Estado constitucional social y democrático de derecho.”<sup>52</sup> Y, en particular señala que las actividades de inteligencia en ese ámbito atenderán cuestiones como el terrorismo, la criminalidad organizada, con especial énfasis en el narcotráfico y la trata de personas.

Dentro de las actividades de inteligencia se incluirá la producción de información vinculada con los “atentados contra el orden constitucional y la vida democrática”. En este grupo de acciones se incluyen, según esta nueva doctrina, las actividades de grupos económicos o financieros que realicen corridas bancarias y cambiarias, desabastecimientos, y que puedan derivar en un “golpe de mercado”.

Siguiendo un análisis preliminar realizado por ADC, puede ser problemático ampliar los “actos de fuerza contra el orden institucional y el sistema democrático” que ya aparecen definidos en la Constitución Nacional dado que “podría incentivar prácticas estatales que podrían derivar en la violación de derechos de la ciudadanía. Los atentados al orden constitucional se encuentran claramente definidos en la Constitución y el poder ejecutivo no debería ampliar esos supuestos por vía reglamentaria.”<sup>53</sup>

Dentro de las funciones que tiene el nuevo organismo encargado de la inteligencia en Argentina y en lo vinculado a seguridad interior, aparece la producción de inteligencia referida a delitos federales complejos como los ciberdelitos, “el uso fraudulento y la difusión ilegal de contenidos.”<sup>54</sup>

Cabe señalar, por lo menos, la vaguedad en las definiciones. Por ejemplo, no se desprende del documento qué se entiende por ciberseguridad, un término, por demás, complejo y problematizado a nivel global en las discusiones sobre regulación y gobernanza de Internet. Este cuerpo doctrinario tampoco da precisiones sobre qué tipo de prácticas podrían caer bajo la muy amplia “difusión ilegal de contenidos.” Por ejemplo, cabe preguntarse si la difusión de contenidos en línea que violan los derechos autorales<sup>55</sup> podría ser una actividad

susceptible de actividades de inteligencia. Todas estas, cuestiones que podrían ser peligrosas en términos de vigilancia y ejercicio de derechos en internet.

### **3.4 Vigilancia de las Comunicaciones en la Normativa de Telecomunicaciones**

#### **3.4.1 Argentina Digital**

El marco regulatorio actual en materia de telecomunicaciones está dado por la ley “Argentina Digital,”<sup>66</sup> aprobada en diciembre de 2014. La aprobación se dió luego de una muy rápida discusión en el Congreso argentino y sin la debida participación de todos los sectores involucrados en este sector clave.<sup>67</sup> Esta nueva ley reemplaza a la normativa anterior de 1972, salvo en las cuestiones que no se opongan a las previsiones establecidas en esta nueva ley.<sup>68</sup>

En cuanto al tema de la vigilancia, la ley “Argentina Digital” establece la inviolabilidad de las comunicaciones realizadas a través de las redes y servicios de telecomunicaciones. Según la ley, la interceptación, así como su posterior registro y análisis, sólo podrá realizarse mediante el requerimiento de un juez competente.<sup>69</sup>

Otro artículo establece las obligaciones para los usuarios de los denominados servicios de tecnologías de la información y comunicación. Esta ley, en su artículo 60, señala que los usuarios de estos servicios deberán permitir el acceso del personal que trabaja en las empresas que proveen los servicios de telecomunicaciones y a la Autoridad Federal de Tecnologías de la Información y la Comunicación (AFTIC). La AFTIC es el organismo público encargado de implementar este marco regulatorio “a los efectos de realizar todo tipo de trabajo o verificación necesaria.”<sup>60</sup>

Organizaciones de la sociedad civil advirtieron, en su momento, que la redacción amplia y vaga de este artículo podría implicar un riesgo a la privacidad de los usuarios e ir a contramano del articulado de la Constitución Nacional que, como mencionamos antes, establece la inviolabilidad del domicilio.<sup>61</sup>

#### **3.4.2 Reglamento de Calidad de los Servicios de Telecomunicaciones**

Otra normativa a tener en cuenta en materia de telecomunicaciones es el Reglamento de Calidad de los Servicios, elaborado por la Secretaría de Comunicaciones en 2013.<sup>62</sup> De acuerdo al nuevo marco normativo dado por Argentina Digital,<sup>63</sup> este organismo, sus funciones y prerrogativas quedan bajo la órbita de la nueva autoridad de aplicación, la Autoridad Federal de Tecnologías de la Información y la Comunicación (AFTIC). Analizaremos los problemas que podría tener este reglamento en materia de vigilancia en el apartado vinculado a retención de datos.

### 3.4.3 Ley 25.891 de Servicios de Comunicaciones Móviles

Esta ley,<sup>64</sup> que si bien no ha sido reglamentada, se encuentra dentro de la normativa vigente de acuerdo al Portal Nacional de Usuarios de Telecomunicaciones, sitio oficial en la materia.<sup>65</sup>

Esta normativa de 2004 instituye un Registro de Usuarios de teléfonos móviles con el objetivo de detectar actividades ilícitas realizadas a través de estos dispositivos. Esta norma ordena la creación de una base de datos para registrar teléfonos móviles perdidos o robados que, además, a la que el Estado puede acceder “de manera inmediata, a toda hora y todos los días del año”, ante requerimiento del Poder Judicial y/o el Ministerio Público.”<sup>66</sup>

La ley va en contra de la normativa de datos personales en tanto los prestadores del servicio de telefonía móvil están obligados a recolectar, retener y divulgar datos personales sin límites ni finalidades establecidos por la ley. La norma, que carece de una definición sobre qué tipo de datos pueden ser solicitados, obliga a las prestadoras de telefonía móvil compartir “toda la información sobre clientes y usuarios” (por la vaguedad del articulado, esto puede contemplar desde datos personales del titular del equipo, el modelo del mismo hasta información sobre las comunicaciones que realiza).

Además, como señalamos, no establece un plazo máximo de retención de datos personales ni prohíbe a los prestadores la transferencia de los mismos o un uso distinto de aquel para el que fueron recolectados.<sup>67</sup>

## 3.5 Normativa sobre Retención de Datos

En Argentina no existe legislación sobre la conservación obligatoria de datos de tráfico por parte de las empresas prestadoras de conexión. Sin embargo, existen algunas cuestiones en el Reglamento de Calidad de los Servicios de Telecomunicaciones antes citado. El reglamento fue elaborado por la antes denominada Secretaría de Comunicaciones.<sup>68</sup> A partir de la aprobación de la ley “Argentina Digital”, este organismo se fusionó con la Comisión Nacional de Comunicaciones convirtiéndose en la nueva Autoridad Federal de Tecnologías de la Información y la Comunicación (AFTIC).

De acuerdo a este reglamento, los prestadores de servicios de telecomunicaciones deberán garantizar el libre acceso de la Comisión Nacional de Comunicaciones (ahora, la Autoridad Federal de Tecnologías de la Información y la Comunicación —AFTIC—) a las instalaciones y sistemas vinculados a la prestación del servicio, y brindar toda la información que les sea requerida en las formas y en los plazos que la ex CNC establezca.<sup>69</sup>

Este reglamento, asimismo, señalaba que este organismo público, a fin de cumplir con los estándares de calidad establecidos en el reglamento, podría “requerir a los prestadores de

servicios de telecomunicaciones la información que estime pertinente, fijando un plazo para su presentación.<sup>70</sup> El reglamento, agrega que, a fin de implementar el sistema de evaluación de la calidad del servicio, los prestadores deberán proveer a la autoridad de aplicación “el libre acceso a sus redes y a su información.”<sup>71</sup>

Si bien, más adelante, la resolución indica que la medición de la calidad del servicio deberá efectuarse en concordancia con el marco de protección de los datos personales,<sup>72</sup> estos artículos tienen, cuanto menos, una redacción confusa que podría llevar a un trato inadecuado de los datos de los usuarios<sup>73</sup> y echaría por tierra lo antes mencionado sobre la necesidad que exista una autorización judicial en el marco de una investigación.

Y, específicamente, en cuanto a retención de los datos, el artículo 8 de este reglamento, señala que los prestadores de telecomunicaciones deben conservar, en archivos electrónicos y por un plazo mínimo de tres años, los datos recogidos por sus sistemas que sirvieran de base para el cálculo de los indicadores de calidad establecidos por esta normativa. Asimismo, señala que la autoridad de aplicación podrá requerir “la entrega total o parcial de los mismos y proceder a su almacenamiento durante el lapso que considere conveniente,”<sup>74</sup> aspecto que consideramos discrecional y que podría ser contrario a los estándares internacionales.

### **3.6 Reglas para el Allanamiento del Domicilio y Registro y Secuestro de Equipos Informáticos**

Como explicaremos más adelante, los códigos de procedimiento son dictados en cada jurisdicción, por lo tanto las normas para el procedimiento de allanamiento variarán en cada provincia. Aquí analizaremos el procedimiento contenido en el Código Procesal Penal de la Nación, que se aplica para delitos federales.

#### **3.6.1 Orden de Registro**

Si hubiere motivos para presumir que en determinado lugar existen cosas vinculadas a la investigación del delito o que allí se pueda efectuar la detención del imputado o de alguna persona evadida o sospechada de haber participado de un hecho delictivo, el juez ordenará, a requerimiento de parte y por auto fundado, el registro de ese lugar.<sup>75</sup>

El registro puede ser llevado a cabo personalmente por el representante del Ministerio Público Fiscal, o podrá encomendar la diligencia al funcionario debidamente individualizado del Ministerio Público Fiscal o de la policía u otra fuerza de seguridad que estime pertinente.<sup>76</sup>

### 3.6.2 Allanamiento de Morada

En principio, debe realizarse en horario diurno. Si existiera peligro en la demora, podrá procederse en cualquier horario, explicitando las circunstancias extraordinarias en la orden de allanamiento.<sup>77</sup> El allanamiento será ordenado por el juez y no podrá ser suplido por el consentimiento de quien habita el lugar.<sup>78</sup>

### 3.6.3 Excepciones al Requisito de Orden Judicial

Podrá llevarse a cabo un allanamiento sin orden judicial cuando:

- Por incendio, explosión, inundación u otro estrago se hallare amenazada la vida de los habitantes o la propiedad;
- Mediante denuncia, cuya entidad resulte verosímil de acuerdo a las circunstancias, de que una o más personas han sido vistas mientras se introducían en una casa o local con indicios manifiestos de comisión de un delito;
- Se introdujere en una casa o local algún sospechado de delito a quien se persigue para su aprehensión;
- Voces provenientes de una casa o local pidieren socorro o anunciaren que allí se está cometiendo un delito;
- Se tuvieren sospechas fundadas que en una casa o local se encuentra la víctima de una privación ilegal de la libertad y corre peligro inminente su vida o integridad física; el representante del Ministerio Público Fiscal deberá autorizar la medida.<sup>79</sup>

### 3.6.4 Requisitos que Debe Cumplir la Orden Judicial

El juez examinará el cumplimiento de los requisitos formales y la razonabilidad de los motivos que fundan el pedido del representante del Ministerio Público Fiscal.<sup>80</sup>

La orden debe ser escrita y debe contener:

- La identificación de la investigación en el marco de la cual se libra;
- La indicación detallada del lugar o lugares que habrán de ser registrados;
- La finalidad con la que se practicará el registro.

El día en que la medida deberá efectuarse y, si correspondiera, la habilitación horaria y la descripción de las cosas a secuestrar o personas a detener, así como de la autoridad que la llevará a cabo.

En casos graves y urgentes, la comunicación de la orden a quien se le encomiende el allanamiento podrá realizarse por medios electrónicos o por cualquier otro medio idóneo, con constancia fehaciente sobre el modo de comunicación utilizado y de la identificación del receptor.

Si la solicitud fuese por vía telefónica, el juez exigirá al representante del Ministerio Público Fiscal ciertos requisitos<sup>81</sup> y, si fueran reunidos, autorizará la medida.

### **3.6.5 Formalidades para el Allanamiento**

La orden de allanamiento será comunicada entregándose una copia de ella al que habite o posea el lugar donde deba efectuarse o, cuando esté ausente, a su encargado o, a falta de éste, a cualquier persona mayor de edad que se hallare en el lugar, preferentemente a los familiares del primero.

El funcionario a cargo del procedimiento deberá identificarse e invitar al notificado a presenciar el registro. Cuando no se encontrare ninguna persona, ello se hará constar en el acta.

### **3.6.6 Recaudos para el Allanamiento**

La diligencia se realizará procurando afectar lo menos posible el derecho a la intimidad.<sup>82</sup> El registro se circunscribirá al lugar específico sobre el que se sospecha que pudiera encontrarse el objeto de búsqueda y comprenderá exclusivamente los elementos que estén relacionados con ese fin.

Si en estricto cumplimiento de la orden de allanamiento se encontraren objetos que evidenciaren la comisión de un delito distinto al que motivó la orden, se pondrá en conocimiento del juez o representante del Ministerio Público Fiscal interviniente quien, en caso de estimarlo adecuado, ordenará su secuestro.

En un acta, que será firmada por los concurrentes, se dejará constancia explicativa sobre el lugar y la forma en que fueron hallados todos los objetos secuestrados.

## **3.7 Otras normativas**

### **3.7.1 Normativa de Protección de Datos Personales**

El reconocimiento del derecho de hábeas data y la protección de datos personales aparece, en primer término, y como señalamos antes, dado por la Constitución Nacional en su artículo 43. En cuanto a la protección de datos personales en la legislación argentina, esto se encuentra regulado a partir de la ley 25.326 del año 2000. La referida ley tiene como objetivo la protección integral de los datos personales que se encuentran en bases de datos, tanto públicas como privadas. Su fin es garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que tienen sobre esa información.<sup>83</sup> Junto con esta ley, conforman el marco de protección de datos personales el decreto que la

reglamenta<sup>84</sup>—y sus modificaciones<sup>85</sup>—y la ley 26.343<sup>86</sup> que la modifica en uno de sus artículos.

En su artículo 2, la ley de datos personales señala que se entiende por dato personal a la “información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables”. Y define como dato sensible al dato personal capaz de revelar el origen racial y étnico, las opiniones políticas, las convicciones religiosas, la afiliación sindical, la información referente a la salud o a la vida sexual.

En su artículo 4, esta norma señala que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular y que deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que fueron recolectados.

Siguiendo un trabajo elaborado por ADC, el marco legal argentino, a pesar de ofrecer una fuerte protección a los datos personales presenta “debilidades estructurales”. La primera de estas debilidades, dice ADC, está vinculada a una excesiva permisividad hacia el Estado en relación con el almacenamiento, tratamiento y cesión de los datos personales.<sup>87</sup>

La ley 25.326 establece la prohibición de tratar y de ceder datos personales sin el consentimiento de los titulares. Sin embargo, el artículo 5 que exige ese consentimiento permite evadirlo cuando estos se recaban “para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.” En otras palabras, la garantía del consentimiento es inútil cuando quien recaba información es el Estado.

El artículo 11 impide la cesión de los datos si el titular de los mismos no ha prestado su consentimiento. Pero—nuevamente—ese requisito puede ser dejado de lado cuando lo disponga una ley, cuando los datos hayan sido recabados para el ejercicio de funciones propias de los poderes del Estado o cuando la cesión se realice entre dependencias de los órganos del Estado en forma directa en la medida del cumplimiento de sus respectivas competencias.

Como vemos, la ley de datos personales mediante estas excepciones, redactadas en términos amplios, permite al Estado evadir la prohibición de tratar o ceder datos con el consentimiento de su titular. Al hacerlo, priva a los ciudadanos de la principal herramienta de defensa de la privacidad de sus datos.<sup>88</sup>

El otro inconveniente del marco regulatorio argentino en materia de datos personales tiene que ver ciertos problemas de origen en cuanto a su diseño institucional de la autoridad de aplicación de esta ley. La Dirección Nacional de Protección de Datos Personales, que funciona dentro de la órbita del Ministerio de Justicia y Derechos Humanos, es un órgano de control débil y dependiente del Poder Ejecutivo.<sup>89</sup>

### 3.7.2 Sistemas de Registro y Recolección de Datos y Vigilancia

Argentina es un país pionero en materia de políticas vinculadas a la identificación de su ciudadanía a partir de técnicas biométricas,<sup>90</sup> entendidas como técnicas que permiten el reconocimiento automático de las personas en base a características biológicas y de comportamiento.<sup>91</sup> Si bien no está vinculado estrictamente a la vigilancia de las comunicaciones, es pertinente a fin de tener un panorama más amplio de la situación en Argentina, dar cuenta de cómo en los últimos años, a partir de la incorporación de nuevos sistemas digitales de recolección y registro de datos por parte de distintos organismos públicos, se ha producido una notable expansión en estas capacidades de vigilancia del Estado argentino.

Diversas organizaciones de derechos humanos vienen llamando la atención sobre el rumbo que está tomando esta recolección, almacenamiento y uso de los datos personales.<sup>92</sup> Estas preocupaciones tienen que ver, en gran medida, con la escasa información oficial acerca de qué hace el Estado con esos datos recabados, por cuánto tiempo los almacena, cómo los analiza, quién tiene acceso a ellos, con qué fines y qué tipo de cruces se realizan entre las distintas bases de datos de estos organismos públicos.<sup>93</sup>

Estos cuestionamientos se relacionan con las observaciones realizadas en secciones anteriores sobre la ley de datos personales en Argentina y dos de sus inconvenientes: (i) que el consentimiento no es necesario cuando los datos personales se recaban para el ejercicio de las funciones propias del Estado o en virtud de una obligación legal y (ii) que habilita a los distintos organismos públicos a compartir entre sí datos personales.<sup>94</sup>

En los últimos años se ha demostrado, además, el uso inadecuado de datos sensibles publicados sin autorización y con una finalidad distinta a la requerida, en contradicción con la normativa de datos personales.<sup>95</sup>

### 3.7.3 Documento Nacional de Identidad

En la Argentina el Documento Nacional de Identidad (de ahora en más, DNI) es el único instrumento de identificación personal. Por ley,<sup>96</sup> el DNI—que incluye elementos biométricos, como la fotografía y la huella digital del pulgar<sup>97</sup>—es obligatorio para todos los ciudadanos y residentes extranjeros.<sup>98</sup> En Argentina, es necesario presentar esta identificación para todo tipo de interacción: desde un trámite ante un organismo público hasta para la realización de transacciones bancarias o compras con tarjeta de crédito.

A partir del decreto 1501/2009<sup>99</sup> y de distintas resoluciones del Registro Nacional de las Personas (RENAPER),<sup>100</sup> se comenzó a expedir en 2009 un nuevo DNI, confeccionado íntegramente por el Estado argentino. El nuevo DNI incorpora tecnologías informáticas en

el proceso de su producción: datos biográficos y huellas en bases de datos digitalizados, y procesos de verificación dactiloscópica mediante herramientas informáticas.<sup>101</sup>

El año pasado, el Ministro del Interior anunció un nuevo “DNI inteligente” que, gracias a un chip, permitirá “interactuar con todos los servicios”, desde los datos del Sistema Único de Boleto Electrónico (que se explicará en el siguiente apartado), pasando por la Administración Nacional de la Seguridad Social hasta las historias clínicas de los ciudadanos argentinos.<sup>102</sup>

Según un trabajo de Laura Siri que recopila información oficial sobre este documento “inteligente”, el Estado argentino, de esta manera, hará un uso más eficiente y tendrá un acceso más seguro a información y datos que hoy están dispersos. Siri señala que el Ministerio del Interior y Transporte, a través del RENAPER, será el organismo que tendrá a su cargo la recolección, almacenamiento, evaluación, destrucción y procesamiento de los datos del nuevo DNI.<sup>103</sup>

Diversos organismos de derechos humanos se manifestaron, en el último tiempo, en contra de esta iniciativa que permitiría al DNI “pasar a convertirse en una base de datos portable y digitalizada con datos biológicos, biográficos y de la rutina diaria de transporte y consumo, que podrán actualizarse y monitorearse en tiempo real.”<sup>104</sup>

### **3.7.4 Sistema Único de Boleto Electrónico**

Mediante una resolución de 2010,<sup>105</sup> se creó el Sistema Único de Boleto Electrónico (SUBE) que permite utilizar el transporte público. A partir del uso de una tarjeta que se registra con todos los datos personales,<sup>106</sup> este sistema genera un registro de todos los viajes que realizan los usuarios, creando así una base de datos controlada por Secretaría de Transporte de la Nación.<sup>107</sup>

Entre los problemas que muestra este sistema, podemos señalar que los datos personales vinculados a los viajes que realizan los usuarios son accesibles no sólo para la persona titular de la tarjeta. Por ejemplo, ingresando el número de la tarjeta en la página oficial de SUBE, y sin necesidad de ingresar ninguna contraseña, se podrá acceder a los registros de viajes que el usuario en cuestión haya realizado con la tarjeta. Esto iría en contra de lo establecido en la ley de datos personales.<sup>108</sup>

Asimismo, este sistema ha demostrado vulnerabilidad en cuanto al resguardo de la información personal de la ciudadanía.<sup>109</sup>

### **3.7.5 Sistema Federal de Identificación Biométrica**

El Sistema Federal de Identificación Biométrica (SIBIOS) fue creado en 2011 a través de un decreto presidencial<sup>110</sup> sin debate público ni discusión parlamentaria. Los objetivos de

SIBIOS, según el decreto que le da origen, tienen que ver con brindar una mayor seguridad y prevenir el delito.

SIBIOS, que depende del Ministerio de Seguridad, es un sistema de identificación biométrica centralizado y con cobertura nacional que permite a las agencias de seguridad hacer “referencias cruzadas” de información con datos biométricos y otros datos, inicialmente, recogidos por el RENAPER. La principal fuente de información de SIBIOS es la base de datos de este organismo, tal como lo establece el artículo 2 del decreto que crea este sistema.

SIBIOS, siguiendo lo que sostiene ADC en uno de sus trabajos, representa un cambio significativo en el Registro Nacional de las Personas. Los objetivos del documento nacional de identidad ahora pasan a ser herramientas clave en la política criminal del Estado argentino. Hasta el surgimiento de SIBIOS, sostiene ADC, la relación entre las fuerzas de seguridad y el Registro Nacional de las Personas era indirecta: si la Policía Federal quería acceder a información del RENAPER debía solicitar ese acceso. Ahora con este sistema, la base de datos de SIBIOS será accesible para las fuerzas de seguridad federales (Policía, Gendarmería, Prefectura y Policía aeroportuaria) así como la Dirección Nacional de Migraciones y el RENAPER.<sup>111</sup>

El artículo 3 del decreto 1176/2011 promueve que las provincias se adhieran, lo que implicaría que las fuerzas de seguridad provinciales podrían acceder a una única base de datos para poder realizar “consultas biométricas en tiempo real.”<sup>112</sup> Según analiza el periodista Claudio Savoia en un libro publicado recientemente sobre vigilancia en Argentina, en la actualidad, ya adhirieron al sistema y comparten sus bases de datos quince provincias argentinas y, hasta septiembre de 2014 fecha de los últimos datos consolidados, ya contaba con 13,2 millones de registros de huellas dactilares.<sup>113</sup>

SIBIOS representa, señala la ADC en uno de sus trabajos, la consolidación de bases de datos que estaban dispersas y la ampliación del acceso a las fuerzas de seguridad del Estado.<sup>114</sup> Este sistema, además, va en contra de la ley de datos personales, que establece que los datos no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.<sup>115</sup>

### **3.7.6 Disposiciones de la Dirección Nacional de Datos Personales**

Como señalamos antes, la Dirección Nacional de Protección de Datos Personales (DNPDP), dependiente del Ministerio de Justicia y Derechos Humanos, es el organismo encargado de la aplicación de la ley de datos personales. En el último tiempo, la DNPDP ha publicado una serie de normas reglamentarias y, algunas de ellas, algunas relacionadas con el tema de vigilancia.

### 3.7.7 Recolección de datos personales a través de VANTs o drones

La disposición 20/2015<sup>116</sup> entiende, siguiendo a la ley de datos personales, que una imagen, registro fílmico o sonoro de una persona constituye un dato de carácter personal y que, por lo tanto, debe estar comprendido por ese marco regulatorio. Esta disposición regula, en particular, la actividad de los Vehículos Aéreos No Tripulados (VANTs) o drones en cuanto a su capacidad de recolectar información.<sup>117</sup> Esta preocupación viene despertando el interés de las organizaciones de derechos humanos en tanto su utilización puede plantear graves amenazas al derecho a la privacidad, entre otros.<sup>118</sup>

La disposición señala que los VANTs o drones<sup>119</sup> realizan “una peculiar” recolección de datos personales que “podrían implicar un importante riesgo para los derechos a la privacidad y a la autodeterminación informativa.”<sup>120</sup>

En el Anexo I de esta disposición, se detallan las “Condiciones de licitud para la recolección de datos personales a través de drones”. El primero de los artículos de este anexo, señala que la recolección de datos personales (ya sean fotográficos, fílmicos, sonoros o de cualquier otra naturaleza) a través de drones será lícita en tanto se realice con el consentimiento del titular del dato, en línea con los artículos 5 y 6 de la ley de datos personales.

De todas formas, señala la disposición, no será necesario el consentimiento del titular de los datos, (i) siempre que los medios para la recolección de la información no impliquen “una intromisión desproporcionada en la privacidad”, (ii) cuando los datos se recolecten en un acto público y (iii) si la recolección de los datos la realiza el Estado nacional “en el ejercicio de sus funciones”. Esto último, en línea con lo que establece la Ley Nacional de Datos Personales que, como señalamos anteriormente, otorga excesivas prerrogativas al Estado en su capacidad de recolectar datos de la ciudadanía.

En el artículo 2, la disposición señala, en relación con el tratamiento de los datos recolectados por drones, que estos deben ser proporcionados, pertinentes y no excesivos respecto de la finalidad con la que fueron recabados y verificando que no afecten el derecho a la intimidad. Y agrega que los responsables del tratamiento de recolección de los datos personales a través de los drones deberán contar con un manual de tratamiento de datos personales y privacidad que indique, entre otras cosas, la finalidad de la recolección, el plazo de conservación de los datos, y los mecanismos técnicos de seguridad y confidencialidad previstos a fin de dar cumplimiento a lo que establece el marco regulatorio de datos personales.

El artículo 3 por su parte, exige la inscripción de las bases de datos generadas por la actividad de los drones o VANT ante el Registro Nacional de Datos y el artículo 5 contiene una excepción que deja fuera del ámbito de aplicación de la disposición a lo que tiene que ver con “fines recreativos”.

La disposición también señala que se deberán extremar las precauciones para no recolectar datos sensibles. Por esta razón, señala la norma, deberá evitarse la captura de información personal en establecimientos de salud, lugares de culto, manifestaciones políticas o sindicales, entre otros.

### 3.7.8 Disposición sobre Videovigilancia

El uso de cámaras con fines de seguridad es una tendencia creciente en Argentina.<sup>121</sup> Según datos oficiales del primer semestre de este año, en la ciudad de Buenos Aires y los municipios del Conurbano bonaerense funcionan alrededor de 12.600 cámaras.<sup>122</sup> La regulación de la videovigilancia se encuentra comprendida por distinta normativa a nivel provincial. Por ejemplo, la ley 2.602 que regula la videovigilancia en la Ciudad Autónoma de Buenos Aires,<sup>123</sup> la ley 13.164 de Santa Fe,<sup>124</sup> la ley 9.380 en Córdoba, la ley 5.984 sobre videograbaciones de seguridad de Corrientes, entre otras.

Esta disposición de la DNPDP establece, a nivel nacional, las condiciones de licitud para las actividades de recolección y tratamiento de imágenes digitales con fines de seguridad.

En su artículo 1, esta disposición sigue la línea de la normativa general de protección de datos personales al señalar que la recolección de imágenes digitales, a través de cámaras de seguridad, será lícita en la medida que cuente con el consentimiento previo e informado del titular del dato.

Nuevamente, en esta disposición encontramos excepciones para esto. La disposición establece que, siempre y cuando la recolección de las imágenes personales no implique una “intromisión desproporcionada” en la privacidad, no será necesario el consentimiento previo en un evento privado. En otras palabras, el consentimiento previo no será necesario cuando la recolección de los datos es efectuada por parte del organizador del evento o, como venimos analizando, la recolección sea realizada por el Estado en el ejercicio de sus funciones. Tampoco será necesario el consentimiento cuando se recolecten dentro de un predio de uso propio como, por ejemplo, una propiedad privada, un espacio alquilado o concesionado.

En su artículo 2, esta disposición—al igual que la normativa que venimos analizando—señala que las imágenes no podrán ser utilizadas para una finalidad distinta o incompatible a la que motivó su captación. Y que el Estado, “sólo podrá disponer su difusión al público cuando se encuentre autorizado por ley o por decisión del funcionario competente y medie un interés general que lo justifique”. Y, como en otras normas emanadas por este organismo, señala que la información recabada debe ser adecuada, pertinente y no excesiva en relación a la finalidad para la que se hubiera obtenido y deberá evitarse, especialmente, cualquier afectación a la privacidad.

La disposición señala que las imágenes captadas que atenten contra los derechos de las personas deberán ser eliminadas a pedido del titular del dato.

Los responsables de las actividades de recolección y posterior tratamiento de imágenes digitales de personas con fines de seguridad, deberán contar con una política de tratamiento de datos personales y privacidad. La política deberá determinar el tiempo por el cual resultará de utilidad el registro de las imágenes, y eliminarse, una vez vencido ese plazo.<sup>125</sup> También debe poner en práctica las condiciones de licitud previstas en la ley 25.326.<sup>126</sup>

Como en el caso de la información recabada a través de drones, las bases de datos en las que se almacenan datos personales obtenidos mediante cámaras de seguridad deberán inscribirse en el Registro Nacional de Bases de Datos.<sup>127</sup>

### **3.7.9 Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones**

En este documento orientativo, la Dirección Nacional de Datos personales busca establecer pautas en relación a la protección de los datos personales sobre la aplicación de políticas de privacidad en el desarrollo de aplicaciones.<sup>128</sup>

El documento resalta la capacidad de las aplicaciones de recabar, usar y transferir información de carácter personal y resalta la importancia del “dato”, como algo que, sin importar dónde está almacenado o cómo se esté utilizando, es propiedad de su titular. Y, señala, que el titular del dato tiene derecho a controlar los usos que se le da a su información personal.<sup>129</sup>

En el apartado 2 dedicado a los principios de privacidad, el documento señala que el consentimiento del titular para el uso de su información personal es la única manera en la que el tratamiento de datos sea lícito, salvo que se trate de las excepciones antes mencionadas que contempla el marco regulatorio.

Este documento orientativo insta a los diseñadores de aplicaciones a ser claros sobre el uso de sus datos y qué tipo de usos se hará, y a poner en práctica los principios de *privacy by design* y *privacy by default*. También insta a los desarrolladores a establecer una política de privacidad.

Como en las disposiciones antes mencionadas, el documento orientativo establece que los datos recolectados sólo pueden ser utilizados de acuerdo a la finalidad por la que fueron obtenidos. Estos no deben ser excesivos en relación a la finalidad que motivaron su recolección ni obtenidos por medios desleales o fraudulentos. Finalmente, deben ser destruidos cuando hayan dejado de ser útiles.<sup>130</sup>

## 4.

### Jurisprudencia

En 2009, la Corte Suprema de Justicia de la Nación se pronunció en el fallo “Halabi”, la sentencia más importante en materia de vigilancia de comunicaciones.

En 2004 se promulgó una norma que modifica la Ley de Telecomunicaciones. Con el objetivo de combatir delitos, se agregaron tres artículos que obligaban a los prestadores de servicios de comunicaciones de disponer de los recursos necesarios para la ‘captación y derivación de las comunicaciones para su observación remota a requerimiento del Poder Judicial o del Ministerio Público’, y de conservar esa información por diez años. Estos artículos fueron reglamentados por un decreto, que un año más tarde fue suspendido.<sup>131</sup> Si bien la reglamentación estaba suspendida, la ley que ordenaba la interceptación de las comunicaciones seguía vigente.

Ernesto Halabi era un abogado que inició una acción de amparo, solicitando la inconstitucionalidad de estos tres artículos, sobre la base que violaba el derecho a su privacidad e intimidad y, además, le impedía garantizar a sus clientes el secreto profesional.

El caso finalmente llegó a la Corte Suprema, que se pronunció sobre el tema. El máximo tribunal sostuvo que todo lo datos sobre las comunicaciones que los individuos transmiten por las vías pertinentes integran la esfera de intimidad personal. Estos datos sobre las comunicaciones se encuentran alcanzadas por las previsiones constitucionales que protegen la privacidad y establecen la inviolabilidad del domicilio, y lo dispuesto en la Declaración Universal de Derechos Humanos y la Convención Americana de Derechos del Hombre.<sup>132</sup>

Respecto de las facultades del Estado para garantizar la seguridad y mantener el orden público, citó a la Corte Interamericana de Derechos Humanos en el caso “Bulacio”, en cuanto sostuvo que la actuación de los Estados está limitada por los derechos fundamentales de los individuos.<sup>133</sup>

La Corte Suprema entonces sostuvo que solamente podría justificarse la intromisión en la vida privada de una persona cuando la intromisión esté prevista en una ley, y siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen.<sup>134</sup>

La Corte citó fallos anteriores sobre los supuestos en los que podría restringirse válidamente la inviolabilidad de la correspondencia:

- que haya sido dictada una ley que determine los "casos" y los "justificativos" en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia;
- que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión;
- que la aludida restricción resulte un medio compatible con el fin legítimo propuesto, y
- que dicho medio no sea más extenso que lo indispensable para el aludido logro. A su vez, fines y medios deberán sopesar con arreglo a la interferencia que pudieran producir en otros intereses concurrentes.<sup>135</sup>

Respecto de los artículos cuestionados, la Corte consideró que no respetaban los supuestos arriba citados en los que podría restringirse válidamente la inviolabilidad de la correspondencia. Los artículos no precisaban las oportunidades ni las situaciones en las que operara las interceptaciones, ni previó un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales.<sup>136</sup> Por todas estas razones, la Corte declaró la inconstitucionalidad de estos artículos.

## 5.

### Marco Institucional

#### 5.1 Organigrama de los Órganos Involucrados en la Persecución Penal

Para desarrollar esta sección, es necesario hacer una aclaración previa. Argentina adoptó para su gobierno la forma federal.<sup>137</sup> Un Estado federal supone la existencia de más de un centro territorial con capacidad normativa. Se equilibra la unidad de un Estado con la pluralidad y la autonomía de las provincias.<sup>138</sup>

La Constitución Nacional delega en el Congreso Nacional la legislación sustantiva o de fondo: Códigos Civil, Comercial, Penal, de Minería, y del Trabajo y Seguridad Social. Sin embargo, establece que la aplicación corresponderá a los tribunales federales o provinciales, según si las cosas o las personas cayeren bajo sus respectivas jurisdicciones.<sup>139</sup> El objetivo es mantener una unidad y coherencia en cuanto al derecho de fondo, para evitar contradicciones, y al mismo tiempo respetar la autonomía de las provincias para delinear los códigos procesales para implementar ese derecho de fondo.

Esto quiere decir que el Código Penal es sancionado por el Congreso Nacional y se aplica en todo el país. Las provincias no podrían dictar sus propios códigos penales. Mientras que la reglamentación de estos códigos de fondo como los códigos procesales deberán ser dictados por cada jurisdicción.

Por todo esto, es difícil describir de forma precisa el marco de actores y órganos involucrados en la persecución penal de Argentina, y realizar un diagrama del procedimiento para interceptar una comunicación, ya que ambos aspectos irán variando según la jurisdicción que se analice. En todo caso, tomaremos como modelo el Código Procesal Penal Federal, que se aplica para delitos con jurisdicción federal ya que, a su vez, muchas de las regulaciones provinciales siguen el criterio del código federal.

#### ***Órganos involucrados en la persecución penal de su país***

##### ***A. Órganos jurisdiccionales:<sup>140</sup>***

- Jueces con funciones de revisión;
- Jueces con funciones de juicio;

- Tribunales de Jurados;
- Jueces con funciones de garantías;
- Jueces con funciones de ejecución.

B. *Ministerio Público Fiscal.*<sup>141</sup> Tiene a su cargo la investigación de los delitos y la promoción de la acción penal pública contra los autores y partícipes.

- Fuerzas de seguridad.

C. *Defensoría General de la Nación.*

## 5.2 Diagrama de Proceso Penal Para Interceptar una Comunicación

El Código Procesal Penal Nacional establece el siguiente procedimiento para interceptar una comunicación:

- El juez podrá ordenar, a petición de parte, la interceptación y secuestro de correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a éste, si tal interceptación resulta útil para la comprobación del delito.<sup>142</sup> Se procederá de modo análogo al allanamiento.
- La intervención de comunicaciones tendrá carácter excepcional y sólo podrá efectuarse por un plazo máximo de treinta (30) días. Este plazo puede renovarse si se expresan motivos que justifiquen la extensión del plazo conforme la naturaleza y circunstancias del hecho investigado.<sup>143</sup>
- La solicitud para intervenir comunicaciones debe indicar el plazo de duración que se estime necesario según las circunstancias del caso.<sup>144</sup>
- El juez debe controlar la legalidad y razonabilidad del requerimiento, y resolver fundadamente.
- Aquellos funcionarios encargados de efectuar la intervención tienen un deber de confidencialidad y secreto respecto de la información obtenida por estos medios, excepto respecto de la autoridad que la haya requerido. Si se incumple este deber de confidencialidad, el funcionario incurrirá en responsabilidad penal.<sup>145</sup>
- Las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal.<sup>146</sup>
- Debe interrumpirse la interceptación si los elementos de convicción tenidos en consideración para ordenar la medida desaparecieran, o una vez que hubiere transcurrido su plazo de duración o ésta hubiere alcanzado su objeto.

### 5.2.1 Incautación de Datos

- El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación.<sup>147</sup>
- El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó.<sup>148</sup>
- Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos.<sup>149</sup>
- El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos.<sup>150</sup>

### 5.2.2 Apertura de los Efectos Interceptados

- Una vez recibida la correspondencia o los efectos interceptados, el representante del Ministerio Público Fiscal procederá a su apertura. Examinará los objetos y leerá el contenido de la correspondencia.<sup>151</sup>
- El representante del Ministerio Público Fiscal debe explicar, en una audiencia unilateral, los fundamentos por los cuales solicita mantener el secuestro de los objetos que tuvieran relación con el proceso.<sup>152</sup>
- Sobre el resto de los efectos, el juez mantendrá la reserva del contenido y dispondrá la entrega al destinatario o a sus representantes o parientes próximos, bajo constancia.<sup>153</sup>

Por otro lado, la Ley 25.520 de Inteligencia Nacional establece que la Agencia Federal de Inteligencia tiene la potestad de producir inteligencia criminal. Eventualmente puede solicitar la interceptación de comunicaciones referida a los delitos federales complejos relativos a terrorismo, narcotráfico, tráfico de armas, trata de personas, cibercrimitos. También puede hacerlo contra delitos atentatorios del orden económico y financiero, así como delitos contra los poderes públicos y el orden constitucional, con medios propios de obtención y reunión de información. Este proceso se desarrollará más adelante.

## 5.3 Organigrama de los Órganos Inteligencia

A partir de la recientemente aprobada la ley 27.126 que modifica a la Ley de Inteligencia Nacional, el sistema de inteligencia en Argentina está constituido, en primer lugar por la Agencia Federal de Inteligencia (AFI).

La AFI es la autoridad máxima en materia de inteligencia en Argentina y dirige al resto de los organismos que lo integran.<sup>154</sup> La AFI depende, directamente, del Poder Ejecutivo

Nacional—de hecho, la autoridad superior del Sistema de Inteligencia Nacional es el Presidente de la Nación y es quien tiene a su cargo la formulación de la política de Inteligencia Nacional.<sup>155</sup> La AFI es conducida por un Director General, con rango de ministro cuya designación está a cargo del Poder Ejecutivo con acuerdo del Senado.<sup>156</sup>

Según la Nueva Doctrina de Inteligencia Nacional, una normativa reciente que complementa a la ley 27.126 y da lineamientos en materia de inteligencia, las funciones de la AFI tienen que ver con:

- La producción de inteligencia nacional mediante la obtención, reunión y análisis de la información referida a los hechos, riesgos y conflictos que afecten la defensa nacional y la seguridad interior, a través de los organismos que forman parte del sistema de inteligencia nacional.
- La producción de inteligencia criminal referida a los delitos federales complejos relativos a terrorismo, narcotráfico, tráfico de armas, trata de personas, cibercrimes, y atentatorios contra el orden económico y financiero, así como los delitos contra los poderes públicos y el orden constitucional, con medios propios de obtención y reunión de información.<sup>157</sup>

Los otros organismos que componen el sistema de inteligencia argentino son:

- La Dirección Nacional de Inteligencia Criminal (DINICRI), que depende del Ministerio de Seguridad.<sup>158</sup> La DINICRI tiene como función la producción de inteligencia criminal,<sup>159</sup> salvo la vinculada a delitos federales complejos o delitos contra los poderes públicos y el orden constitucional. Estas funciones fueron transferidas directamente a la AFI.<sup>160</sup>
- La Dirección Nacional de Inteligencia Estratégica Militar (DINIEM), dependiente del Ministerio de Defensa de la Nación.<sup>161</sup> La DINIEM tiene a su cargo la producción de inteligencia estratégica operacional y la inteligencia táctica necesarias para el planeamiento y conducción de operaciones militares y de la inteligencia técnica específica.<sup>162</sup>

## **5.4 Proceso de los Cuerpos de Inteligencia para Interceptar Comunicaciones**

De acuerdo al artículo 4 de la ley 27.126 que modifica la Ley de Inteligencia Nacional, “las actividades de inteligencia serán ordenadas por las máximas autoridades de cada organismo”. Este artículo agrega, sin embargo que, “en caso de urgencia” estas actividades “podrán ser iniciadas, debiendo ser informadas de manera inmediata a las autoridades máximas de cada organismo de inteligencia”.

A la hora de realizar interceptaciones en las comunicaciones privadas, la AFI, el organismo máximo del Sistema Nacional de Inteligencia desde la ley 27.126, debe solicitar la autorización judicial.<sup>163</sup> Esta autorización, señala el marco normativo, “deberá formularse por escrito y estar fundada indicando con precisión el o los números telefónicos o direcciones electrónicas o de cualquier otro medio, cuyas comunicaciones se pretenda interceptar o captar.”<sup>164</sup>

La autorización judicial será requerida al juez federal penal con competencia jurisdiccional por el Director General de la AFI o el funcionario en quien se delegue esta facultad. La jurisdicción se establece de acuerdo al domicilio de las personas físicas o jurídicas cuyas comunicaciones van a ser interceptadas o desde la sede donde se realizarían, en caso que se trate de comunicaciones móviles o satelitales.

La autorización para la interceptación de comunicaciones será concedida por un plazo no mayor de 60 días que caducará automáticamente, salvo que, ante el pedido formal del Director de la AFI o del funcionario que esté ejerciendo esa facultad, el juez otorgue una extensión del plazo por otros 60 días como máximo (siempre que sea imprescindible para completar la investigación).<sup>165</sup>

Una vez que se vencen estos plazos, el juez ordenará la iniciación de la causa correspondiente o, en caso contrario, la destrucción de los elementos que permitan dar cuenta del resultado de las interceptaciones.<sup>166</sup>

Con la aprobación de la ley 27.126, la antes denominada Dirección de Observaciones Judiciales (DOJ), el único órgano del Estado encargado de llevar adelante interceptaciones o captaciones de comunicaciones privadas, se transfirió al ámbito de la Procuración General de la Nación del Ministerio Público, un órgano independiente con autonomía funcional y autarquía financiera. A partir de este traspaso, la DOJ pasó a denominarse Departamento de Interceptación de Captación de las Comunicaciones (Dicom).<sup>167</sup>

Las órdenes judiciales para la interceptación de las comunicaciones telefónicas serán enviadas a la Dicom con instrucciones precisas para orientar dicha tarea (por ejemplo, los números a ser intervenidos). Después, la Dicom debe enviar ese pedido a la empresa de servicios telefónicos responsable de ejecutar la derivación de la comunicación.

Con estas nuevas normativas, no sólo se transfirió a la Procuración General el sistema operativo, sino también las bases de datos informáticas y los archivos documentales del organismo anterior con el material de las intervenciones concluidas al momento del traspaso.

En este sentido, señala la normativa, se creará una Comisión de Administración de Registros de Intervenciones Concluidas y se pondrán bajo su custodia los archivos vinculados a intervenciones de comunicaciones finalizadas antes del traspaso.

El proceso para la interceptación de una comunicación quedaría de esta forma:

- AFI
- Autorización judicial (juez federal penal con jurisdicción)
- Ministerio Público Fiscal,<sup>168</sup> Procuración General de la Nación<sup>169</sup>
- Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal (DATIP)
- Departamento de Interceptación de Captación de las Comunicaciones (DICOM)

## 6.

### Formas de Control

#### 6.1 Entidades Autorizadas Para Intervenir Una Comunicación Privada Sin Orden Judicial

De acuerdo con la normativa penal y la normativa de actividades de inteligencia desarrolladas en secciones anteriores, no podría interceptarse una comunicación sin un orden judicial.

#### 6.2 Obligación de Reportes de Transparencia y Supervisión Pública

En el proceso penal de interceptación de comunicaciones no se prevé una obligación de realizar reportes de transparencia. En el proceso de inteligencia, se contempla la obligación del órgano de inteligencia de elaborar informes anuales secretos de actividades de inteligencia, que debe presentar ante la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia.<sup>170</sup> A continuación, desarrollaremos las funciones que debe llevar a cabo esta Comisión de supervisión.

##### 6.2.1 Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia

Este órgano de control parlamentario fue creado en 2001, cuando se promulgó la Ley de Inteligencia Nacional 25.520. Según esta ley, las funciones de la Comisión incluyen supervisar a los organismos del Sistema de Inteligencia Nacional, fiscalizar su funcionamiento para que se ajuste estrictamente a las normas constitucionales y legales, y controlar a las actividades de inteligencia.<sup>171</sup> Esto último abarca la consideración, análisis y evaluación de la ejecución del Plan de Inteligencia Nacional; la consideración del Informe Anual de las Actividades de Inteligencia; la elaboración y remisión en forma anual al Poder Ejecutivo Nacional y al Congreso de la Nación de un informe secreto sobre el análisis y evaluación de las actividades, funcionamiento y organización del Sistema de Inteligencia Nacional en función de la ejecución del Plan de Inteligencia Nacional, entre otras funciones.<sup>172</sup> La ley otorga a la Comisión “amplias facultades para controlar e investigar de oficio”. Sin embargo, la ley impone una limitación, en tanto “el acceso a dicha información será autorizado en cada caso por el Presidente de la Nación o el funcionario en quien se delegue expresamente tal facultad, con las excepciones previstas en la presente ley.”<sup>173</sup> Esta disposición supedita el control de la Comisión a la voluntad del mismo controlado.<sup>174</sup>

La Comisión comenzó a funcionar en 2004, cuando se le asignaron fondos para comenzar sus funciones.<sup>175</sup> En la práctica, se ha afirmado que funciona con un total secretismo, hasta en las cuestiones que no son, o no deberían ser secretas.<sup>176</sup> Por ejemplo, en su página web, no figura información sobre las reuniones de la Comisión ni su agenda de trabajo.<sup>177</sup>

A fines de diciembre de 2012, un grupo de organizaciones de la sociedad civil, parte de la Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI), presentaron un pedido de acceso a la información ante la Comisión Bicameral.<sup>178</sup> En ese documento, solicitaron información sobre las reuniones de la Comisión, copias de los informes realizados por la Comisión que no sean secretos, si ha realizado investigaciones de oficio en relación a presuntas irregularidades en el ejercicio de la actividad de inteligencia, entre otras cuestiones. A pesar de haber sido reiterado dos veces, el pedido no ha sido respondido hasta el cierre de este informe.<sup>179</sup>

En febrero de 2015 se reveló que la Comisión se reunió a puertas cerradas para analizar el proyecto de reforma a la Ley de Inteligencia.<sup>180</sup>

Asimismo, en la resolución que da origen a la Dicom, se constituye una comisión asesora, denominada Comisión de Implementación, integrada por expertos en la materia y, por otro lado, se insta a la creación en el Congreso de una comisión bicameral del Ministerio Público que funcione como una instancia de control externo sobre el funcionamiento del DICOM.

En la misma resolución, se señala que habrá un consejo consultivo de instituciones dedicadas a estas temáticas a fin de que den recomendaciones, buscar mecanismos para asegurar la transparencia y participarán en debates, como el del protocolo.

### **6.3 Mecanismos de Notificación Diferida**

Tanto el proceso penal como el procedimiento de inteligencia para interceptar comunicaciones privadas carecen de un mecanismo de notificación diferida al usuario afectado.

En el proceso penal, solamente en los casos de allanamiento, o de incautación de un sistema informático, el afectado recibe una notificación. Sin embargo, en los casos de interceptación de comunicaciones privadas, si esas comunicaciones interceptadas no terminan utilizándose en una causa penal, el afectado podría no enterarse nunca de que su comunicación fue interceptada.

## 7.

### **Aplicación de la Ley y Diseños Institucionales**

A lo largo de los últimos años, han tenido lugar en Argentina distintos episodios relacionados con la vigilancia e interceptación de las comunicaciones. Espionaje a e-mails de periodistas y jueces.

Por ejemplo, en 2006 y a raíz de una investigación periodística trascendió públicamente que se habían violado correos electrónicos de periodistas y jueces.<sup>181</sup> Este hecho tuvo un impacto en lo que después fue la promulgación de la ley 26.388, que incorporó al Código Penal muchos de los delitos informáticos desarrollados previamente.

Si bien había habido numerosos intentos previos similares para modificar el Código para incluir estos delitos, fue este episodio específico el que aumentó el impulso de esta ley en tanto la violación de correos electrónicos, en ese entonces, no estaba tipificada. Esta situación puso en evidencia los vacíos que tenía el Código Penal en materia de delitos informáticos, y poco después se aprobó la reforma.<sup>182</sup>

#### **7.1 Causa por Escuchas Ilegales en la Ciudad de Buenos Aires**

Este caso reviste gravedad institucional en tanto el jefe de gobierno de la Ciudad de Buenos Aires y actual candidato a presidente, Mauricio Macri, está procesado desde 2010 en esta causa por ser "partícipe necesario de una asociación ilícita" dedicada al espionaje ilegal.<sup>183</sup>

En la decisión del tribunal se responsabiliza al jefe de gobierno porteño por participar del armado de una "estructura de inteligencia subterránea" en la Ciudad de Buenos Aires y se lo imputa por escuchas telefónicas ilegales denunciadas, entre otros, por su ex cuñado y dirigentes de familiares de víctimas de la AMIA opositores al gobierno porteño.<sup>184</sup> En la misma causa, está procesado y aguardando juicio, entre otros, un ex jefe de la Policía Metropolitana de la Ciudad de Buenos Aires.

#### **7.2 Proyecto X**

Uno de los escándalos más grandes del último tiempo en materia de vigilancia. El denominado "Proyecto X", implementando desde 2005 y descubierto en 2012, comprendía actividades de recolección y sistematización de información de inteligencia llevadas adelante por la Gendarmería Nacional. Actividades que, a contramano del marco legal analizado en secciones anteriores, no estaban enmarcadas en ninguna causa judicial, ni autorizadas por un

juez ni se rindió cuenta de ellas ante la Comisión Bicameral encargada de auditar las actividades de inteligencia.

Proyecto X, cuya existencia fue reconocida por la entonces ministra de Seguridad de la Nación como por el jefe de gendarmería, consistía en una base de datos con información sobre organizaciones sociales, ambientalistas, familiares de víctimas de la represión, movimientos sociales, sindicatos y organismos de derechos humanos.<sup>185</sup>

Proyecto X consistía en tareas de espionaje en las que efectivos de Gendarmería que se infiltraban en manifestaciones y en protestas de organizaciones opuestas al Gobierno.<sup>186</sup> A raíz de estas protestas, se realizaban denuncias judiciales contra los manifestantes, basadas en la información aportada por los agentes infiltrados.

El que, según la ex ministra de Seguridad no era espionaje sino, en realidad, “sólo un software”<sup>187</sup> iba en contra, por ejemplo, de la prohibición establecida por la ley de Inteligencia Nacional, antes analizada, que impide a las fuerzas de seguridad la producción de inteligencia o el almacenamiento de datos sobre las personas por su opinión política o por su adhesión o pertenencia a organizaciones sociales, sindicales, partidarias, comunitarias, etc. Asimismo, Proyecto X contradecía el marco jurídico establecido por la ley de protección de datos personales que impide recoger datos “por medios desleales, fraudulentos;”<sup>188</sup> almacenar “datos sensibles”<sup>189</sup> como los que revelan “opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical.”<sup>190</sup>

En la actualidad, existe una causa en trámite vinculada a esta iniciativa en la que se investiga si la tarea ejercida por Gendarmería fue o no ilegal. El expediente se encuentra en la etapa de instrucción y, hasta el momento, no se ha indagado a nadie.

### **7.3 Compra de Equipamiento para Vigilancia de las Comunicaciones**

A raíz de un pedido de información realizado por parlamentarios alemanes, trascendió que Argentina compró a ese país equipamiento para vigilancia electrónica. Este caso da cuenta de la falta de transparencia en relación a las actividades de vigilancia en tanto, hasta ahora, las características, los fines de este equipamiento o qué organismo habría sido su destinatario se mantienen en secreto.<sup>191</sup>

Asimismo, en las recientes filtraciones de WikiLeaks<sup>192</sup> trascendió que existieron contactos con Hacking Team para la posible compra de software de espionaje. De este material se desprende que hubo presentaciones de los productos de la empresa italiana ante organismos públicos argentinos dedicados a tareas de inteligencia. Como en el caso de las compras de

equipamiento, hasta el momento no existe información más concreta ni una declaración oficial al respecto.

## 7.4 La Muerte del Fiscal Nisman y la Reforma al Sistema de Inteligencia

Sin embargo, el caso más reciente ha sido la muerte en enero de 2015 de Alberto Nisman,<sup>193</sup> el fiscal a cargo de la causa por el atentado contra la Asociación Mutual Israelita Argentina (AMIA) en 1994. Nisman, la noche antes de presentarse ante el Congreso para presentar su denuncia contra la Presidenta por encubrimiento en la causa, fue encontrado muerto en su departamento.

Una investigación del experto en seguridad del portal *The Intercept*, Morgan Marquis-Boire, señaló que Nisman fue atacado por un software espía (*malware*)\_descargado en su teléfono celular poco antes de su misteriosa muerte.<sup>194</sup> Marquis-Boire explica que el malware fue ocultado bajo un documento .PDF que decía confidencial y tenía la intención de infectar un ordenador con Windows. Sin embargo, Nisman abrió el archivo desde su teléfono Android por lo cual no llegó a infectarse.<sup>195</sup> Según el diario, *The Intercept*, se desconoce si Nisman abrió el archivo desde su computadora. Agrega Marquis-Boire, que el ataque no fue un hecho aislado y que las persona o personas que aparecen detrás del intento de vigilancia también han ejecutado otras operaciones desde distintos lugares de América del Sur a otros objetivos como el periodista Jorge Lanata.

Una de las consecuencias de la muerte del fiscal fue poner en la mira y en el debate público el funcionamiento de los servicios de inteligencia en Argentina.<sup>196</sup> Poco tiempo después de la muerte del fiscal y en medio de declaraciones de distintos sectores de la política argentina, que asociaban a los servicios de inteligencia con el hecho,<sup>197</sup> la Presidenta presentó, a través de una cadena nacional, un proyecto para reformar el sistema de inteligencia, en tanto “no ha servido a los intereses nacionales”.

Este proyecto dio lugar a los cambios desarrollados en este informe en materia de inteligencia: la disolución de la Secretaría de Inteligencia, la creación de una Agencia Federal de Inteligencia, la transferencia de las escuchas telefónicas a la Procuración Nacional, entre otros.

## 8.

# ¿Respetar Argentina los Estándares Internacionales de Derechos Humanos Frente a la Vigilancia Estatal?

### Legalidad

*Este principio requiere que cualquier limitación a los derechos humanos deba ser prescrita por ley, que deberá ser precisa y clara, para asegurar que las personas la conozcan por adelantado.*

Las interceptaciones a las telecomunicaciones en el régimen penal y de inteligencia deben realizarse conforme a la Constitución Nacional, los tratados de derechos humanos suscriptos por la Argentina y las disposiciones previstas en leyes y códigos. Ambos cuerpos normativos detallan el procedimiento para ordenar la interceptación de una comunicación y qué funcionarios pueden autorizarlas. En este sentido, cumplen con el requisito de legalidad.

Sin embargo, cuestiones que aparecen en el marco regulatorio en materia de inteligencia podrían derivar en acciones discrecionales por parte del Estado. Por ejemplo, la ley de inteligencia nacional establece que son las “autoridades máximas” de cada organismo del sistema de inteligencia las que ordenan estas actividades. De todas formas, señala que “en caso de urgencia” estas actividades podrán iniciarse, debiendo ser informadas de manera inmediata a esas máximas autoridades.<sup>198</sup> Consideramos que el hecho de no definir taxativamente qué se entiende por “caso de urgencia” podría derivar en acciones que vulneren derechos fundamentales.

La misma amplitud y falta de precisión en ciertas definiciones aplica para la nueva doctrina en materia de inteligencia. La nueva doctrina emana de un decreto del Poder Ejecutivo y, por lo tanto, no fue discutido en el Congreso ni hubo debate público al respecto. La nueva doctrina amplía los denominados atentados contra el orden constitucional lo que podría ser problemático en términos de legalidad en tanto no están definidos claramente. La misma falta de precisión se le puede objetar cuando se refiere a las actividades de inteligencia en la investigación por el uso fraudulento y la difusión ilegal de contenidos, por ejemplo.

La actual regulación sobre telecomunicaciones también incluye cuestiones vagas y amplias que podrían ser peligrosas y podrían abrir la puerta a prácticas de vigilancia en las comunicaciones.

La ley “Argentina Digital” establece, por un lado, el marco general en materia de Tecnologías de la Información y Comunicación (TIC). Por otro lado, establece la inviolabilidad de las comunicaciones realizadas a través de las redes y servicios de telecomunicaciones. Y señala que la interceptación de las comunicaciones, así como su posterior registro y análisis, sólo podrá realizarse mediante el requerimiento de un juez competente.<sup>199</sup> Hasta aquí cumple con el principio de legalidad.

Pero, en otro de sus artículos, establece obligaciones para los usuarios de los denominados servicios TIC que podrían ir contra de esa premisa y del principio de legalidad. Como analizamos antes, establece como una obligación que los usuarios deberán permitir el acceso del personal de las empresas que proveen servicios TIC y de la AFTIC “a los efectos de realizar todo tipo de trabajo o verificación necesaria.”<sup>200</sup>

La resolución podría representar un problema para este principio de legalidad en tanto contiene cuestiones muy amplias. Por ejemplo, los prestadores de servicios de telecomunicaciones deberán garantizar “el libre acceso a sus redes y a su información” a la AFTIC, y deberán brindar toda la información que les sea requerida y que este organismo “estime pertinente”.<sup>201</sup>

Lo mismo se puede aplicar a la Ley 25.891 de Servicios de Comunicaciones Móviles. Esta ley obliga a los prestadores de conexión móvil a recolectar, retener y divulgar datos personales sin establecer de manera clara los límites ni las finalidades de la recolección, ni qué tipo de datos se están recolectando. Simplemente obliga a compartir “toda la información sobre clientes y usuarios”.

Por lo menos, cabe señalar que estas normativas no son claras, son amplias, carecen de precisión y podrían avalar procedimientos discrecionales por parte de la autoridad contrarios a los estándares internacionales en materia de privacidad.

### **Objetivo Legítimo**

*Las interceptaciones a las comunicaciones deben estar justificadas de forma que cumplan un objetivo legítimo que corresponda a un interés jurídico preponderante, importante y necesario en una sociedad democrática. Las normas que permiten la vigilancia de las comunicaciones no pueden basarse sobre condiciones como raza, sexo, idioma, religión, opinión política, nacionalidad, entre otros.*

En principio, el régimen legal argentino que prevé interceptaciones a las comunicaciones cumple con este requisito, en tanto establece que las interceptaciones serán realizadas de forma excepcional, con el objetivo de comprobar delitos complejos o de asegurar la defensa nacional y la seguridad interior.

De todas formas, como analizamos antes, el nuevo marco que regula las actividades de inteligencia en Argentina amplía los actos que pueden ser considerados contra el orden institucional y el sistema democrático y que serían objeto de actividades de inteligencia. Como dijimos, esta ampliación podría incentivar nuevas prácticas estatales que podrían ser peligrosas en términos de vigilancia y ejercicio de derechos humanos y pondría en cuestión este principio de objetivo legítimo.

En cuanto al marco de telecomunicaciones, las obligaciones de retención de información por los prestadores de servicios no se encuentran debidamente justificadas. Solo esgrimen motivos como el cálculo de indicadores de calidad y permiten a la autoridad de aplicación conservarlos “por el lapso que considere conveniente.”<sup>202</sup> Tampoco justifica debidamente con qué fines más allá de los antes mencionados estándares de calidad del servicio.

En materia de telecomunicaciones tampoco se cumple con este principio. Esta norma obliga a los usuarios a permitir el acceso de la autoridad de aplicación a los fines de realizar “todo tipo de trabajo o verificación necesaria” sin dar precisiones sobre qué tipo de trabajo, qué tipo de verificación y con qué fines;<sup>203</sup> También obliga a los prestadores de servicios de conexión móviles a informar a la autoridad sobre “toda información” sobre usuarios y clientes del servicio sin dar cuenta cabalmente en el texto de la ley de cuáles serían los fines que justifican este tipo de medidas.<sup>204</sup>

Los nuevos sistemas de recolección de datos analizados en este documento como SUBE, SIBIOS y el DNI, surgidos de normativas que tampoco fueron discutidas públicamente tampoco se ajustan a este principio en tanto no están debidamente justificados sus objetivos. Bajo la muy amplia idea de brindar mayor seguridad, prevenir el delito o simplificar y mejorar los trámites<sup>205</sup> se están recabando y tratando datos biológicos, biográficos y de la rutina diaria de transporte y consumo de la ciudadanía sin mayor transparencia.

Y, más allá que la normativa de datos personales y la de inteligencia prohíben obtener información, producir inteligencia y almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, y opiniones y actividades políticas. Existen ejemplos como el Proyecto X que dan cuenta que esas prácticas sí se implementan por parte de las fuerzas de seguridad en Argentina, a contramano de lo establecido en el marco legal.

## **Necesidad**

*Las interceptaciones a comunicaciones privadas deben realizarse de forma estricta y limitarse a lo necesario para alcanzar dicho objetivo legítimo. Esto significa que la vigilancia debe ser el único medio para alcanzar ese objetivo, o el que menos vulnere derechos humanos.*

En el procedimiento penal para la interceptación de comunicaciones se establece la excepcionalidad de la interceptación de comunicaciones, y el deber del juez de analizar que el requerimiento de interceptación cumpla con la legalidad y la razonabilidad.

El marco legal sobre inteligencia nacional señala que cuando en el desarrollo de las actividades de inteligencia sea “necesario” realizar una interceptación de comunicaciones esta deberá ser solicitada a una autoridad judicial.<sup>206</sup> Pero, en tanto no da más especificaciones sobre cuándo se consideraría “necesario” recurrir a este procedimiento, ni que solicitaron interceptaciones en tanto no existan otros medios que —permitiendo alcanzar los mismos fines— sean menos lesivos para los derechos humanos. En este sentido no se ajustaría a este principio.

De todas formas, el marco de inteligencia establece cuestiones vinculadas a este principio en tanto solo se podrá realizar una interceptación de una comunicación mediante una orden judicial que debe estar formulada por escrito y debe indicar con precisión los números telefónicos o direcciones electrónicas que se pretendan interceptar o captar.<sup>207</sup> La ley de inteligencia nacional también establece que sus actividades se enmarcarán “inexcusablemente” dentro de lo que establece el marco regulatorio de protección de datos personales en Argentina<sup>208</sup> y establece un plazo máximo para la autorización a interceptar una comunicación.<sup>209</sup>

El marco legal en materia de telecomunicaciones reafirma la idea de inviolabilidad de las comunicaciones y que cualquier interceptación deberá realizarse solo con una orden judicial<sup>210</sup> ajustándose a este principio de necesidad, pero normativas que componen el cuerpo legislativo en la materia contradicen este principio en tanto establecen que los prestadores de servicios deberán entregar datos de los usuarios a pedido de la autoridad de aplicación y por el tiempo que esta considere necesario.<sup>211</sup>

### **Adecuación**

*La vigilancia de las comunicaciones prevista en la ley debe ser apropiada e idónea para cumplir el objetivo legítimo específico identificado.*

El régimen de interceptación de comunicaciones en una causa penal prevé la necesidad de que la interceptación sea útil para comprobar un delito.

Por su parte, la regulación de inteligencia se ajusta a este principio al establecer que los datos recabados por medio de las actividades de inteligencia que no sirvan para los fines establecidos por ese marco regulatorio —es decir, la producción de información tendiente a prevenir los riesgos para la seguridad interior y la defensa nacional; y lo que tiene que ver con sus funciones de investigación e inteligencia criminal vinculada a delitos federales

complejos— serán destruidos. La ley de inteligencia señala, asimismo que no se debe almacenar información por motivos de raza, creencias religiosas, acciones privadas, actividades políticas, pertenencia a organizaciones sociales, entre otras.<sup>212</sup>

En materia de telecomunicaciones, como venimos señalando, parte de la legislación que integra el marco normativo no se ajusta por completo a este principio en tanto, no establece un plazo máximo de retención de datos personales.<sup>213</sup> A contramano de lo que sí aparece en la ley de datos personales que, en su artículo 4, señala que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular y que deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que fueron recolectados.

### Proporcionalidad

*Para que la vigilancia de comunicaciones privadas sea proporcional, es necesario que el Estado deba demostrar a una autoridad judicial competente, a los fines de llevar a cabo vigilancia de comunicaciones, ciertos requisitos:*

1. *Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo, y;*

En el ámbito penal este requisito no se cumple en tanto se requiere únicamente que la interceptación resulte útil para la comprobación de un delito, sin especificar si éste debe ser grave.

En lo que tiene que ver con actividades de inteligencia, se pueden solicitar a una autoridad judicial interceptaciones a las comunicaciones dentro del amplio marco de facultades del organismo de inteligencia nacional—desde lo que tiene que ver riesgos para la seguridad interior y la defensa nacional hasta la investigación de delitos federales complejos como narcotráfico hasta corridas bancarias.

2. *Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la Información Protegida, y;*

Este requisito no se cumple en el proceso penal ni en el marco que regula las actividades de inteligencia. En el proceso penal, solamente se exige que la información sea útil, y no que haya sólidos indicios que se accederá a evidencia pertinente. Como señalamos antes, se puede solicitar la captación de comunicaciones en el marco del desarrollo de las actividades

de inteligencia. También mencionamos que es muy amplio el abanico de actividades de inteligencia comprendidas, lo que puede resultar problemático.

3. *Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica. Y;*

Si bien en el ámbito penal se especifica que la interceptación de comunicaciones debe ser excepcional, no se menciona específicamente que haya que agotar otras técnicas de investigación previamente. En cuanto al marco regulatorio en materia de inteligencia, éste tampoco señala que hay que agotar otras técnicas menos lesivas para los derechos humanos.

4. *La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza específica al fin legítimo alegado; y*

En el ámbito penal, la interceptación de comunicaciones se remite a las normas para allanamiento de morada, que prevén limitar el registro exclusivamente a los elementos que estén relacionados con el objeto que se busca. Este principio se cumple en lo que tiene que ver con la regulación de las actividades de inteligencia.

5. *Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud; y*

El régimen penal prevé el deber de confidencialidad y secreto en las interceptaciones de comunicaciones, y en el caso de incautación de datos prevé la devolución de aquellos componentes que no tengan relación con el proceso. La regulación en materia de inteligencia establece un plazo máximo para la interceptación de las comunicaciones y que los datos recabados que no sirvan para los fines establecidos por el marco que regula esta actividad, serán destruidos.<sup>214</sup>

6. *La información será accesada solo por la autoridad específica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización; y*

La normativa penal contempla estos requisitos, en tanto prevé la devolución de los datos incautados y la interrupción de la interceptación una vez cumplido el plazo o cumplido el objetivo.

La normativa de inteligencia se ajusta a este principio en tanto establece que el personal afectado a las actividades de inteligencia, la documentación y los bancos de datos de los organismos de inteligencia “llevarán la clasificación de seguridad que corresponda en interés

de la seguridad interior, la defensa nacional y las relaciones exteriores de la Nación. El acceso a dicha información será autorizado en cada caso por el Presidente de la Nación o el funcionario en quien se delegue expresamente tal facultad”, con las excepciones que prevé esa ley.<sup>215</sup>

Asimismo, se ajusta a este principio en tanto señala que no se deberá almacenar información por motivos de raza, creencias religiosas, acciones privadas, actividades políticas, pertenencia a organizaciones sociales, entre otras.<sup>216</sup>

*7. Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.*

La normativa penal prevé la protección de la privacidad y la intimidad al imponer un deber de confidencialidad a los funcionarios que realizan las intervenciones respecto de la información obtenida, bajo posible responsabilidad penal si lo incumple.

La ley de inteligencia nacional, como se explicó anteriormente, establece sanciones penales para aquellos integrantes de los servicios de inteligencia que indebidamente intercepten, capten o desvíen comunicaciones que no le estuvieran dirigidas.<sup>217</sup>

Por su parte, como vimos, en la normativa de telecomunicaciones, en cuanto a retención de datos incluye cuestiones amplias que pueden derivar en un proceder discrecional por parte de la autoridad de aplicación del marco de Tecnologías de la Información y Comunicación en Argentina. Por ejemplo, normativas que no establecen un plazo máximo de retención de datos personales, permiten un uso distinto de la finalidad con la que fueron recolectados, habilita la cesión de los mismos, entre otros.

### **Autoridad Judicial Competente**

*Este principio establece la necesidad de que las decisiones sobre vigilancia de comunicaciones sean tomadas por una autoridad judicial competente imparcial e independiente. Ésta debe estar separada y ser independiente de las autoridades encargadas de llevar a cabo la vigilancia, debe estar capacitada y ser competente para tomar decisiones judiciales sobre la legalidad de la vigilancia de las comunicaciones, y tener recursos adecuados para el ejercicio de las funciones que se asignen.*

Este requisito se cumple, tanto en el ámbito penal como en el de actividades de inteligencia. Por su parte, en la ley Argentina Digital también se ajusta a este principio en su artículo 5 cuando señala que la interceptación de las comunicaciones sólo podrá tener lugar a requerimiento de un juez competente.

Sin embargo, como se señaló antes este principio no se cumple en artículos de otras leyes que componen el marco regulatorio en materia de telecomunicaciones. Por ejemplo, los reglamentos de calidad del servicio de telecomunicaciones y la ley de servicios de comunicaciones móviles antes mencionados.

### **Debido Proceso**

*Este requisito exige que los Estados respeten y garanticen el ejercicio de los derechos humanos de las personas. Deben asegurar que los procedimientos legales que rigen cualquier interferencia con derechos humanos garanticen una audiencia pública y justa, realizada dentro de un plazo razonable por un tribunal independiente, competente e imparcial. Sólo podría permitirse prescindir de una orden judicial cuando exista un riesgo inminente para la vida humana, y debe subsanarse de forma posterior.*

El régimen penal argentino garantiza, en líneas generales, el debido proceso. Sin embargo, en el caso de un allanamiento, se prevé la posibilidad de realizarlo sin orden judicial en ciertos casos. Estos incluyen casos de amenaza para la vida –caso acorde con este principio- pero además lo permite cuando “una o más personas han sido vistas mientras se introducían en una casa o local con indicios manifiestos de comisión de un delito”. Esta excepción no es del todo precisa y permitiría desnaturalizar el requisito de autorización judicial.

La interceptación de las comunicaciones en el marco de las actividades de inteligencia prevén el debido proceso en tanto sólo pueden realizarse mediante una autorización judicial. Cabe recordar, de todas formas, que el marco regulatorio habilita que se inicien actividades de inteligencia en casos de “urgencia” —que, de todas formas, deberían ser informados de manera inmediata. Esto, consideramos, podría abrir una puerta a la vulneración de derechos en el marco de las actividades de inteligencia.

El marco de inteligencia, asimismo, establece un plazo máximo para la autorización de interceptación de comunicaciones. La autorización se podrá extender por otros 60 días como máximo, siempre que sea imprescindible para completar la investigación.<sup>218</sup>

La retención de datos, siguiendo alguna de las leyes y resoluciones que componen el marco de regulación de las telecomunicaciones no se ajusta del todo a este principio. Si bien, como mencionamos antes, la ley Argentina Digital señala que toda interceptación de las comunicaciones se realizará mediante una orden judicial y en el marco de una investigación, otras normas habilitan a un organismo del Poder Ejecutivo a acceder a datos personales, solicitar información sobre los usuarios y, entre otras cosas, alojarla por el tiempo que considere necesario. Todas estas cuestiones vulneran este principio.

## Notificación del Usuario

*Este principio establece la obligación de notificar al individuo cuyas comunicaciones sean interceptadas, con el tiempo suficiente para impugnar la decisión o buscar otras soluciones. Solamente podría retrasarse la notificación si esto pusiera en serio peligro la finalidad para la que se autoriza la vigilancia, o representa un riesgo inminente de peligro para la vida humana, la autorización para retrasar la notificación es otorgada por la autoridad judicial competente cuando se autoriza la vigilancia, y si se notifica al usuario tan pronto como el riesgo desaparece.*

Este requisito no se cumple en Argentina, ya que no está previsto en el marco normativo penal, ni en el régimen de actividades de inteligencia. No hay una obligación de informar al individuo, ni siquiera una vez concluida la interceptación.

Si de dicha interceptación surjan elementos relevantes para una investigación penal o de inteligencia, el sujeto podría eventualmente enterarse, si dichos elementos son presentados como prueba en un proceso penal. Sin embargo, podría ocurrir que de la interceptación no surgieran elementos relevantes o útiles para la investigación, en cuyo caso el individuo jamás se enteraría que sus comunicaciones fueron vigiladas. '

## Transparencia

*Para cumplir con el requisito de transparencia respecto del alcance y la implementación de las leyes de vigilancia de las comunicaciones, los Estados deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos.*

Este principio tampoco se cumple en el ordenamiento argentino. Si bien los organismos de inteligencia deben elaborar informes para la posterior fiscalización de la Comisión Bicameral, dichos informes no son públicos. Por lo tanto, no hay datos oficiales públicos sobre actividades de interceptación de comunicaciones.

## Supervisión Pública

*Este principio implica que los Estados deben establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones. Estos mecanismos de supervisión deben contar con facultades amplias para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado en cuanto a la vigilancia de comunicaciones.*

*Deben establecerse, además, otros mecanismos de supervisión independientes adicionales a los existentes a través de otra rama del gobierno.*

Es positivo que exista una Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia cuyas amplias facultades de fiscalización permiten asegurar que los órganos que llevan a cabo actividades de inteligencia cumplan con normas constitucionales y respeten derechos humanos. Sin embargo, ésta Comisión ha sido criticada por organizaciones de la sociedad civil por operar con opacidad y secretismo. A pesar de que se han realizado pedidos de información sobre cuestiones de funcionamiento de la Bicameral, éstos no han sido respondidos.

El traspaso, a partir de las recientes modificaciones a la ley de inteligencia nacional, del único órgano del Estado argentino que puede llevar adelante interceptaciones o captaciones de las comunicaciones al ámbito de la Procuración General de la Nación del Ministerio Público, un “órgano independiente con autonomía funcional y autarquía financiera”<sup>219</sup> es un paso positivo en relación con el cumplimiento de este principio.

En este sentido, también se puede mencionar como avances a fines de cumplir con este principio a la comisión asesora que se crea para lo que tiene que ver con la recientemente creada DICOM, el organismo público encargado de las intervenciones telefónicas; que se inste a la creación de una comisión parlamentaria del Ministerio Público que funcione como una instancia de control externo sobre el funcionamiento del DICOM. Y un consejo consultivo de instituciones y organizaciones de la sociedad civil.

Más allá de esto, no se contempla ningún mecanismo adicional independiente para la supervisión de actividades de inteligencia.

### **Integridad de las Comunicaciones y Sistemas**

*Para garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, los Estados no deben obligar a los proveedores de servicios o proveedores de “hardware” o “software” a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado.*

Nunca debe exigirse a priori a los proveedores de servicios la retención o la recopilación de datos. La mencionada Resolución que establece el Reglamento de Calidad de los Servicios de Telecomunicaciones, elaborado por la Secretaría de Comunicaciones, podría representar un problema para este principio.

Este reglamento señala que los prestadores de telecomunicaciones deben conservar, en archivos electrónicos y por un plazo mínimo de tres años, los datos recogidos por sus sistemas que sirvieran de base para el cálculo de los indicadores de calidad establecidos por esta normativa. La autoridad de aplicación podrá luego requerir la entrega de tales datos. Si bien los datos recolectados serán utilizados solamente para los cálculos de indicadores de calidad, y el reglamento contempla el deber de respetar los datos personales, consideramos que esta facultad podría ser contraria a este principio.

Por otro lado, la guía de buenas prácticas en privacidad para el desarrollo de aplicaciones, si bien es orientativa y no es vinculante de la Dirección Nacional de Datos Personales (DNNDP) es un paso positivo con vistas al cumplimiento de este principio en tanto insta a los diseñadores de aplicaciones a ser claros sobre el uso de sus datos y qué tipo de usos se hará y a poner en práctica los principios de *privacy by design* y *privacy by default*.

### **Garantías para la Cooperación Internacional**

*Este principio requiere que los acuerdos de cooperación internacional celebrados por los Estados garanticen que, cuando pueda aplicarse la legislación de más de un Estado, se adopten los estándares más protectores para las personas. Dichos acuerdos deben incluir también el principio de doble incriminación.*

Si bien debe analizarse cada acuerdo en particular, ante la falta de un acuerdo de cooperación específico, la ley de cooperación internacional en materia penal dispone el requisito de doble incriminación para que proceda la extradición de una persona.

### **Garantías contra el Acceso Ilegítimo**

*Este principio prevé que los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los “whistleblowers” y medios de reparación a las personas afectadas.*

*Además, las leyes deben establecer que después de que el material obtenido a través de la Vigilancia de las Comunicaciones ha sido utilizado con la finalidad por el que fue obtenida la información, el material no debe ser retenido, en su lugar, debe ser destruido o devuelto a los afectados.*

Consideramos positivo que en el ámbito penal y en el de actividades de inteligencia se prevé la pena para la interceptación ilegal de comunicaciones o realización ilegal de actividades de inteligencia, con penas agravadas en caso de funcionarios públicos.

Respecto de la protección a los informantes o “whistleblowers”, la normativa penal que criminaliza la publicación de comunicaciones privadas prevé una excepción para quienes hubieran obrado con “el propósito inequívoco de proteger un interés público.”<sup>220</sup>

Por su parte, la Ley 25.520 de Inteligencia Nacional incorporó este año disposiciones penales para castigar a quien, participando en forma permanente o transitoria de las tareas reguladas en dicha ley, “indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos.”<sup>221</sup>

Esta ley también tipifica el delito de quien, con orden judicial y estando obligado a hacerlo, “omitire destruir o borrar los soportes de las grabaciones, las copias de las intervenciones postales, cablegráficas, de facsímil o de cualquier otro elemento que permita acreditar el resultado de las interceptaciones, captaciones o desviaciones.”<sup>222</sup> Siguiendo lo que establece esta normativa, se castiga también a todo funcionario o empleado público que realice acciones de inteligencia prohibidas por las leyes.<sup>223</sup>

Por otra parte, en la normativa de inteligencia nacional no hay incentivos para que los agentes de inteligencia den a conocer públicamente información sobre prácticas que vulneran derechos fundamentales.<sup>224</sup>

## 9.

# Recomendaciones

### En cuanto a la legalidad

- El marco que regula las actividades de inteligencia debería precisar y acotar ciertas definiciones en lo que tiene que ver con atentados contra el orden constitucional a fin de no infringir este principio y que esto derive en prácticas de vigilancia contrarias a los estándares internacionales.
- En cuanto al ámbito de las telecomunicaciones, deben ser revisadas normativas y artículos de la ley Argentina Digital que permitirían un uso de los datos personales de los usuarios contrario al marco de protección de los mismos.

### En cuanto a la proporcionalidad

- Es necesario que la vigilancia de las comunicaciones se limite, como lo establece el principio de proporcionalidad, a delitos graves y prever, expresamente, que primero deben agotarse otras técnicas de investigación menos invasivas.

### En cuanto al debido proceso

- Es necesario acotar más las situaciones en las que se puede realizar un allanamiento sin autorización judicial. Las excepciones tan amplias desnaturalizan el debido proceso.

### En cuanto a notificación del usuario

- Una de las reformas más necesarias es la incorporación de notificación al usuario cuyas comunicaciones son interceptadas.

### En cuanto a la transparencia

- No hay datos oficiales públicos sobre actividades de interceptación de comunicaciones. Es necesario que el Estado publique reportes con, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos.
- A los fines de este propósito, es clave que se pongan en funcionamiento las instancias de supervisión y control previstas en el marco normativo de las actividades de inteligencia.
- Si bien excede lo que tiene que ver con vigilancia de las comunicaciones, es

imprescindible transparentar lo que tiene que ver con los sistemas de recolección de datos como SIBIOS, SUBE y el DNI, entre otros. Hasta el momento, es prácticamente nula la información oficial acerca de qué hace el Estado con esos datos recabados, quién tiene acceso a ellos, con qué fines, de qué manera esos datos se están cruzando, por cuánto tiempo se los almacena, etc.<sup>225</sup>

- Estos cuestionamientos se relacionan con las observaciones realizadas en secciones anteriores sobre la ley de datos personales en Argentina y dos de sus inconvenientes: que el consentimiento no es necesario cuando los datos personales se recaban para el ejercicio de las funciones propias del Estado o en virtud de una obligación legal y que habilita a los distintos organismos públicos a compartir entre sí datos personales.<sup>226</sup>

### **En cuanto a la supervisión pública**

- Es necesario que la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Inteligencia actúe con más transparencia respecto de las cuestiones que no son secretas y, además, deben contemplarse otros mecanismos de supervisión independientes adicionales.

### **En cuanto a garantías contra el acceso ilegítimo**

- A la luz de casos como las revelaciones de Edward Snowden, sería clave que la normativa de inteligencia nacional incorpore incentivos y medidas de protección para los agentes de inteligencia den a conocer públicamente información sobre prácticas que vulneran derechos fundamentales.<sup>227</sup>

- 1 Corte Suprema de Justicia de la Nación, “Ekmekdjian, Miguel Ángel c. Sofovich, Gerardo y otros”, 7 de julio de 1992.
- 2 El artículo 75 inciso 22 incluye a los siguientes tratados de derechos humanos, ratificados antes de 1994: Declaración Americana de los Derechos y Deberes del Hombre; la Declaración Universal de Derechos Humanos; la Convención Americana sobre Derechos Humanos; el Pacto Internacional de Derechos Económicos, Sociales y Culturales; el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo; la Convención sobre la Prevención y la Sanción del Delito de Genocidio; la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial; la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer; la Convención contra la Tortura y otros Tratos o Penas Crueles, Inhumanos o Degradantes; la Convención sobre los Derechos del Niño. El artículo contempla un procedimiento en el Congreso para incorporar a los tratados que se firmen con posterioridad.
- 3 Ley No. 24.767 de Cooperación Internacional en Materia Penal, B.O. del 16/01/1997, artículo 6.
- 4 Ley No. 25.304, B.O. del 07/09/2000.
- 5 *Ibíd.*, artículo 2.1.
- 6 Ley No. 25.911, B.O. del 13/09/1996.
- 7 Conforme a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, el término “comunicaciones” abarca las actividades, interacciones y transacciones transmitidas por medios electrónicos, tales como el contenido, la identidad de las partes, información de rastreo de ubicación incluyendo direcciones IP, momento y duración de las comunicaciones, e identificadores de los equipos utilizados, y “vigilancia de las Comunicaciones” en el entorno moderno comprende monitorear, interceptar, recoger, analizar, usar, preservar, conservar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas.
- 8 Constitución Nacional, artículo 19.
- 9 *Ibíd.*, artículo 18.
- 10 CSJN, “Halabi, Ernesto c/ PEN ley 25.873 y decreto 1563/04 s/ amparo”, sentencia del 24 de febrero de 2009. Disponible en: <http://www.cij.gov.ar/nota-615-La-Corte-reconoce-accion-colectiva-y-da-alcance-general-a-un-fallo.html>
- 11 Constitución Nacional, artículo 43.
- 12 *Ibíd.*
- 13 Aprobado por Ley No. 27.063, promulgada el 9 de diciembre de 2014. La ley No. 27150, promulgada el 17 de junio de 2015, establece un procedimiento gradual de entrada en vigor. A partir de marzo de 2016, el Código entrará en vigor en el ámbito de la justicia nacional. En el ámbito de la justicia federal, entrará en vigor de conformidad con un cronograma de implementación progresiva que establecerá una Comisión Bicameral de Monitoreo e Implementación del Nuevo Código Procesal Penal de la Nación. Ver página web de la Comisión Bicameral. Disponible en: <http://www.senado.gov.ar/parlamentario/comisiones/info/379>
- 14 Artículo 13. El subrayado es nuestro.
- 15 Código Penal, artículo 153.
- 16 *Ibíd.*, artículo 153 bis.

- 17 *Ibíd.*, artículo 155.
- 18 *Ibíd.*, artículo 157 bis.
- 19 Ley No. 25.520 de Inteligencia Nacional, B.O. del 6/12/2001, artículo 42. Disponible en: <http://www.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm>
- 20 *Ibíd.*, artículo 43.
- 21 *Ibíd.*, artículo 43 ter.
- 22 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19.
- 23 Ley No. 27.126 de creación de la Agencia Federal de Inteligencia, B.O. del 05/03/2015. Disponible en: <http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm>
- 24 Decreto No. 337/2015 que promulga la Ley No. 27.126, B.O. del 3/3/2015. Disponible en: <http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243822/norma.htm>
- 25 Decreto No. 950/2002, B.O. del 06/6/2002. Disponible en: <http://www.infoleg.gov.ar/infolegInternet/anexos/70000-74999/74896/norma.htm>
- 26 Decreto 1311/15, B.O. del 6/07/ 2015. Disponible en: <http://www.infoleg.ov.ar/infolegInternet/verNorma.do?id=248914>
- 27 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 1.
- 28 *Ibíd.*, artículo 2.
- 29 Ley No. 23.554 de Defensa Nacional, B.O. del 13/04/1988. Disponible en: <http://www.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm>
- 30 Ley No. 24.059 de Seguridad Interior, B.O. del 17/01/1992. Disponible en: <http://www.infoleg.gov.ar/infolegInternet/anexos/0-4999/458/texact.htm>
- 31 Asociación por los Derechos Civiles, “Quién vigila a quienes vigilan. Estudio comparativo sobre sistemas de control de los organismos de inteligencia”, 2014, p. 5 y 6.
- 32 Ley No. 23.554 de Defensa Nacional, artículo 15.
- 33 Ley No. 24.059 de Seguridad Interior, artículo 8, punto 2.
- 34 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 3.
- 35 Durante el proceso de discusión que se mantenga este aspecto ha sido criticado por organizaciones de derechos humanos. Por ejemplo, el Centro de Estudios Legales y Sociales (CELS) ha señalado: “Este artículo habilitó que durante todos estos años se cuele la actuación de la Secretaría de Inteligencia en cualquier causa judicial como auxiliar de la justicia, lo que alimentó la relación promiscua con sectores importantes de la justicia federal. Si se sostiene esta posibilidad, fracasarán los objetivos de la reforma”. Ver más en Centro de Estudios Legales y Sociales, “Ley de Inteligencia: las reformas al proyecto no solucionan problemas de fondo”, 7 de febrero de 2015. Disponible en: <http://cels.org.ar/comunicacion/?info=detalleDoc&ids=4&lang=es&ss=46&idc=1896>
- 36 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 4.

- 37 *Ibíd.*, artículo 5 bis.
- 38 *Ibíd.*, artículo 18.
- 39 *Ibíd.*
- 40 *Ibíd.*, artículo 41.
- 41 Ley No. 25.326 de Protección de los Datos Personales. B.O. del 13/04/1988. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>
- 42 Ley No. 25.520, *supra* nota 19, artículo 16 quáter., incorporado por el artículo 13 de la ley No. 27.126.
- 43 *Ibíd.*, artículo 16 quinquies, incorporado por el artículo 14 de la ley No. 27.126.
- 44 Ley No. 25.520, *supra* nota 19, artículo 16 sexies, incorporado por el artículo 15 de la ley No. 27.126.
- 45 *Ibíd.*, artículo 42.
- 46 Decreto No. 1311/15, B.O. del 6/07/2015. Disponible en: <http://www.infojus.gob.ar/descarga-archivo?guid=noprstuvwnov-edad-esde-c13112015pdf&name=dec13112015.pdf>
- 47 *Ibíd.*
- 48 Según la nueva doctrina de inteligencia nacional, la “información de inteligencia” es la que comprende “el conjunto de observaciones y mediciones obtenido o reunido de fuentes públicas o reservadas referido a un evento o problemática relevante del ámbito de la defensa nacional o la seguridad interior o que tiene incidencia en esas esferas”.
- 49 *Ibíd.*
- 50 Decreto No. 15, *supra* nota 46, Anexo I. Disponible en: <http://www.boletinoficial.gov.ar/Displaypdf.aspx?s=A&tid=4921811&i=1>
- 51 *Ibíd.*
- 52 *Ibíd.*
- 53 Asociación por los Derechos Civiles, “Observaciones al decreto 1311/15”, 9 de julio de 2015, p. 2. Disponible en: <http://www.adc.org.ar/wp-content/uploads/2015/07/Apuntes-sobre-el-decreto-1311-15.pdf>
- 54 Decreto No. 1311/15, *supra* nota 46, Anexo I.
- 55 Cabe señalar que Argentina cuenta con un marco regulatorio muy restrictivo en cuanto a derechos de autor dado por la Ley de Propiedad Intelectual No. 11.723 del año 1933 que tuvo posteriores modificaciones siempre en sentido más restrictivo.
- 56 Ley No. 27.078 Argentina Digital, B.O. del 19/12/2014. Disponible en: <http://www.infoleg.gov.ar/infolegInternet/anexos/235000-239999/239771/norma.htm>
- 57 Ver más en Fontanals, Gustavo, “La política detrás de AFTIC”, *Bastión Digital*, 13 de julio de 2015. Disponible en: <http://ar.bastiondigital.com/notas/la-politica-detras-de-aftic> y Massare, Bruno y Pautasio, Leticia, “Argentina Digital en

- detalle: qué cambios plantea la nueva ley de telecomunicaciones”, *Infotechnology*, 8 de mayo de 2015. Disponible en: <http://www.infotechnology.com/internet/Argentina-Digital-en-detalle-que-cambios-plantea-la-nueva-ley-de-telecomunicaciones-20150508-0008.html#sthash.UuPMbB3U.dpuf>
- 58 La ley Argentina Digital en su artículo 89 señala que la Ley No. 19.798 y sus modificatorias sólo subsistirán “respecto de aquellas disposiciones que no se opongan a las previsiones de la presente ley”.
- 59 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 5.
- 60 *Ibíd.*, artículo 60, punto d.
- 61 Asociación por los Derechos Civiles, “Alerta de la ADC sobre el proyecto de ley Argentina Digital”, 16 de noviembre de 2014. Disponible en: <http://www.adc.org.ar/alerta-de-la-adc-sobre-el-proyecto-de-ley-argentina-digital/>
- 62 Secretaria de Comunicaciones, Resolución No. 5/2013, 1/7/2013. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm>
- 63 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 87.
- 64 Ley No. 25.891 de Servicios de Comunicaciones Móviles, B.O. del 28/04/ 2004. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/95000-99999/95221/norma.htm>
- 65 Portal Nacional de Usuarios de Telecomunicaciones. Autoridad Federal de Tecnologías de la Información y las Comunicaciones. Disponible en: <http://www.quenosecorte.gob.ar/>
- 66 Ley No. 25.891 de Servicios de Comunicaciones Móviles, Art. 3.
- 67 Vargas, Paula, “Vigilancia masiva de las comunicaciones: inconstitucionalidad de la Ley 25.891”, *Blog Derecho de Internet y Tecnología de las Comunicaciones*, 12 de agosto de 2015. Disponible en: <http://www.ditc.com.ar/2015/08/12/397/>
- 68 Ministerio de Planificación Federal, Inversión Pública y Servicios, Secretaria de Comunicaciones, Resolución No. 5/2013, 1/7/2013. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm>
- 69 *Ibíd.*, artículo 2.
- 70 *Ibíd.*, artículo 3.
- 71 *Ibíd.*, artículo 5, punto 2.
- 72 *Ibíd.*
- 73 Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), “Internet en Argentina: ¿cómo estamos hoy?”, p. 18. Disponible en: <http://www.palermo.edu/cele/pdf/investigaciones/Mapping-ARG-CELE.pdf>
- 74 Ministerio de Planificación Federal, Inversión Pública y Servicios, Secretaria de Comunicaciones, Resolución No. 5/2013, 1/7/2013, artículo 8.
- 75 Código Procesal Penal de la Nación. Artículo 132.
- 76 *Ibíd.*
- 77 Código Procesal Penal de la Nación, artículo 133.

- 78 *Ibíd.*
- 79 *Ibíd.*, artículo 135.
- 80 *Ibíd.*, artículo 137.
- 81 Requisitos establecidos en el artículo 136: a) La determinación concreta del lugar o los lugares que deberán ser registrados; b) La finalidad del registro, mencionando los objetos a secuestrar o las personas a detener; c) El nombre del representante del Ministerio Público Fiscal responsable del control o de la ejecución de la medida, los motivos que fundan su necesidad y cuáles son las evidencias disponibles que, prima facie, la justifican; d) En su caso, los motivos que fundamentan la necesidad de efectuar la diligencia fuera del horario diurno; e) La firma del representante del Ministerio Público Fiscal que requiere la autorización.
- 82 Código Procesal Penal de la Nación, artículo 139.
- 83 Ley No. 25.326 de Protección de los Datos Personales, *supra* nota 41, artículo 1.
- 84 Decreto No. 1558/2001, B.O. del 29/11/2001. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70368/texact.htm>
- 85 Decreto No. 1160/10, B.O. del 11/08/2010. Disponible en: <http://www.infoleg.gov.ar/infolegInternet/anexos/170000-174999/170508/norma.htm>
- 86 Ley No. 26.343, B.O. del 09/01/2008. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/135000-139999/136483/norma.htm>
- 87 Asociación por los Derechos Civiles, “El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos”, 2014, p. 3.
- 88 *Ibíd.*, p. 3 y 4.
- 89 *Ibíd.*, p. 3 y Torres, Natalia, *Acceso a la información y datos personales: una vieja tensión, nuevos desafíos*, Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Universidad de Palermo. Disponible en: [http://www.palermo.edu/cele/pdf/DatosPersonales\\_Final.pdf](http://www.palermo.edu/cele/pdf/DatosPersonales_Final.pdf)
- 90 Véase, Asociación por los Derechos Civiles, “Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina”, mayo de 2015, p. 5. Disponible en: <http://www.adc.org.ar/wp-content/uploads/2015/05/InformeBiometriaADC2015.pdf> y Fascendini, Flavia y Roveri, Florencia, “Tu software, mi biología. Sistemas de vigilancia masiva en Argentina”, *GISWatch Report*, 2014. Disponible en: <http://www.giswatch.org/node/4951>
- 91 Savoia, Claudio, *Espiados*, Buenos Aires, Editorial Planeta, 2015, p. 333.
- 92 Madres de Plaza de Mayo Línea Fundadora, Fundación Vía Libre, Liga por los Derechos del Hombre y otros, “Los DNI electrónicos violan nuestros derechos”, 06 de octubre de 2014. Disponible en: <http://www.pensamientopenal.org.ar/dni/>
- 93 Siri, Laura, “El Documento Nacional de Identidad Argentino: una “caja negra” y una política de veridicción”, III Simposio Internacional LAVITS Vigilancia, Tecno Políticas y Territorios 13-15, mayo 2015. Río de Janeiro, Brasil. Red de Estudios Latinoamericanos sobre Vigilancia, Tecnología y Sociedad (LAVITS), p. 3.
- 94 *Ibíd.*

- 95 Véase también, Villa, Emiliano y Álvarez Ugarte, Ramiro, “Las fotos de los argentinos, al mejor postor”, Boletín *Digital Rights*, 22 de noviembre de 2013. Disponible en: <http://www.digitalrightslac.net/es/las-fotos-de-los-argentinos-al-mejor-postor/>
- 96 Ley No. 17.671 de Identificación, registro y clasificación del potencial humano nacional, BO del 29/02/1968. Disponible en: <http://www.infoleg.gov.ar/infolegInternet/anexos/25000-29999/28130/texact.htm>
- 97 Siri, Laura, *supra* nota 94, p. 2.
- 98 ADC, *supra* nota 91, p. 8.
- 99 Decreto No. 1501/2009, B.O. del 20/10/2009. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/155000-159999/159070/norma.htm>
- 100 RENAPER, Resoluciones No. 585/2012 y No. 797/2012.
- 101 ADC, *supra* nota 74, p. 9.
- 102 “Randazzo anunció nuevo DNI inteligente que incorpora un chip”, Audiovisual Télam, 27 de junio de 2014. Disponible en: <http://www.telam.com.ar/multimedia/video/5091-randazzo-anuncio-nuevo-dni-inteligente-que-incorpora-un-chip/>
- 103 Siri, Laura, *supra* nota 77, p. 5.
- 104 Madres de Plaza de Mayo Línea Fundadora y otros, *supra* nota 76.
- 105 Secretaría de Transporte, Resolución 162/2010, del 27/10/2010. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/170000-174999/170118/norma.htm>
- 106 Es posible usar la tarjeta sin registrarse pero, en caso de no hacerlo, no hay modo de reclamar el saldo no usado si la tarjeta, por ejemplo, se extravía. Asimismo, el uso de esta tarjeta no es obligatorio pero, de no hacerlo, el costo de los viajes es mayor.
- 107 Fundación Vía Libre, “Con SUBE sí vas a pagar más caro: el fin de la privacidad”. Disponible en: <http://www.vialibre.org.ar/2012/01/27/con-sube-si-vas-a-pagar-mas-carro-el-fin-de-la-privacidad/>
- 108 Ley No. 25.326 de Protección de los Datos Personales, *supra* nota 41, artículo 9.
- 109 “Exponen en la Red los registros de viajes de la tarjeta SUBE”, *La Nación*, 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> y “Anonymous SUBE viajes”, *Página 12*, 31 de enero de 2012. Disponible en: <http://www.pagina12.com.ar/diario/cdigital/31-186566-2012-01-31.html>
- 110 Decreto No. 1766/2011.
- 111 ADC, “Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina”, 2015, p. 18.
- 112 Decreto No. 1176/2011, artículo 4.
- 113 Savoia, Claudio, *supra* nota 92, p. 335 y 336.
- 114 ADC, 2015, “Si nos conocemos más, nos cuidamos mejor. Informe sobre políticas de biometría en la Argentina”, p. 17 y 18.

- 115 Tordini, Ximena, “El triunfo final sobre el anonimato”, Revista Crisis, Número 8, febrero-marzo de 2012. Disponible en: <http://www.revistacrisis.com.ar/el-triunfo-final-sobre-el.html>
- 116 Dirección Nacional de Protección de Datos Personales, Disposición No. 20/2015, B.O. 27/05/2015.
- 117 La Administración Nacional de Aviación Civil emitió regulación general sobre los vehículos no tripulados. Véase, ANAC, Resolución N° 527/2015, Reglamento Provisional de los Vehículos Aéreos no Tripulados. Disponible en: <http://www.anac.gov.ar/anac/web/index.php/1/1196/noticias-y-novedades/reglamento-provisional-de-los-vehiculos-aereos-no-tripulados-vant>
- 118 Por ejemplo, organizaciones de la región expusieron sobre el uso de drones y su impacto en los derechos humanos en las Américas en una audiencia ante la Comisión Interamericana de Derechos Humanos en 2013.
- 119 La disposición define, en su Anexo II, al VANT o dron como un artefacto “equipado con cámaras, micrófonos, gps, o cualquier otro tipo de sensor, tiene la capacidad para recolectar datos de personas, como pueden ser imágenes, videos, conversaciones, geolocalización, entre otros. A ello se le suma su capacidad de vuelo, que le permite acceder a lugares a los que el ojo humano no llega; y la posibilidad de operar sin ser detectados”.
- 120 Dirección Nacional de Protección de Datos Personales, Disposición No. 20/2015, B.O. 27/05/2015. Disponible en: [http://www.jus.gob.ar/media/2898655/disp\\_2015\\_20.pdf](http://www.jus.gob.ar/media/2898655/disp_2015_20.pdf)
- 121 Ministerio de Justicia y Derechos Humanos, Dirección Nacional de Protección de Datos Personales, Disposición 10/2015, Bs. As., 24/2/2015. Disponible en: <http://www.infoleg.gob.ar/infolegInternet/anexos/240000-244999/243335/norma.htm>
- 122 Savoia, Claudio, *supra* nota 92, p. 318.
- 123 Ley No. 2.602, 06/12/ 2007.
- 124 Ley No. 13.164.
- 125 *Ibíd.*, artículo 3.
- 126 *Ibíd.*, artículo 7.
- 127 *Ibíd.*, artículo 6.
- 128 Ministerio de Justicia y Derechos Humanos, Dirección Nacional de Protección de Datos Personales, Disposición 18/2015, Bs. As., 10/4/2015. Disponible en: <http://infoleg.mecon.gov.ar/infolegInternet/anexos/245000-249999/245973/norma.htm>
- 129 *Ibíd.*, Introducción.
- 130 *Ibíd.*, Anexo I, Punto 3.
- 131 El Decreto No.357/2005 suspendió la aplicación del Decreto No. 1563.
- 132 Halabi, considerando 23.
- 133 *Ibíd.*, considerando 24.
- 134 Halabi, considerando 24.

- 135 *Ibíd.*, considerando 25.
- 136 *Ibíd.*, considerando 26.
- 137 Constitución Nacional, artículo 1.
- 138 Gelli.
- 139 Constitución Nacional, artículo 75, inciso 12.
- 140 Código Procesal Penal Nacional, artículo 52.
- 141 Código Procesal Penal Nacional, artículo 88.
- 142 Código Procesal Penal Nacional, artículo 143.
- 143 *Ibíd.*
- 144 *Ibíd.*
- 145 *Ibíd.*
- 146 *Ibíd.*
- 147 Código Procesal Penal Nacional, artículo 144.
- 148 *Ibíd.*
- 149 *Ibíd.*
- 150 *Ibíd.*
- 151 Código Procesal Penal Nacional, artículo 145.
- 152 *Ibíd.*, artículo 145.
- 153 *Ibíd.*
- 154 Ley No. 27.126 de creación de la Agencia Federal de Inteligencia, *supra* nota 23, artículo 7.
- 155 Decreto No. 1311/15, *supra* nota 46, Anexo I, Capítulo III.
- 156 Ley No. 27.126 de creación de la Agencia Federal de Inteligencia, *supra* nota 23, artículo 8.
- 157 *Ibíd.*
- 158 Presidencia de la Nación de Argentina. Ministerio de la Seguridad. Disponible en: <http://www.minseg.gob.ar/>
- 159 Decreto No.1311/15, *supra* nota 46, Anexo I, Capítulo III, folio 27.

- 160 Ley No. 27.126 de creación de la Agencia Federal de Inteligencia, *supra* nota 23, artículo 7.
- 161 *Ibíd.*
- 162 Decreto No. 1311/15, *supra* nota 46, Anexo I, Capítulo III, folio 28.
- 163 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 18.
- 164 *Ibíd.*
- 165 *Ibíd.*, artículo 19.
- 166 *Ibíd.*, artículo 20.
- 167 Ministerio Público Fiscal, Resolución, PGN No. 2067/15, 07 de julio de 2015.
- 168 El Ministerio Público Fiscal es parte fundamental en la administración de justicia, compuesta por el Poder Judicial y los Ministerios Públicos: Fiscal y de la Defensa. En su conjunto, conforman las tres partes fundamentales en un proceso judicial. Asimismo, el Ministerio Público Fiscal es un órgano independiente dentro del sistema de administración de justicia. Se encuentra a cargo del Procurador o de la Procuradora General, que es propuesto o propuesta por el Poder Ejecutivo y aprobado por el Congreso de la Nación. Es independiente incluso del Poder Judicial (encabezado por la Corte Suprema de Justicia). Esa independencia tiene sus orígenes en la Reforma Constitucional de 1994, que estableció la autonomía del Ministerio Público. En relación con la parte penal, el Procurador o la Procuradora a cargo del Ministerio tienen la facultad de definir cómo se persiguen determinados delitos que pueden tener una relevancia mayor en la defensa de los intereses generales de la sociedad. Por ejemplo, aquellos que atentan contra la vida, contra la humanidad, los vinculados al narcotráfico, a la violencia institucional, o al lavado de dinero, por mencionar algunos. Por eso es que en la estructura del MPF se conformaron unidades especializadas, que tienen como fin mejorar el desempeño en el trabajo. El Ministerio Público Fiscal de la Nación, es según la ley que le da origen, un órgano autónomo e independiente del Poder Ejecutivo. *Véase también*, Ley No. 27.148 Orgánica del Ministerio Público Fiscal, junio de 2015. Disponible en: <http://www.infojus.gob.ar/27148-nacional-ley-organica-ministerio-publico-fiscal-lns0006116-2015-06-10/123456789-oabc-defg-g6i-16000scanyel>
- 169 La Procuración General es la sede de actuación del/la Procurador/a General de la Nación, jefe del Ministerio Público Fiscal de la Nación y el responsable de su funcionamiento. Su autoridad se extiende a todo el territorio nacional y es designada/o por el Poder Ejecutivo nacional con acuerdo del Senado por dos tercios (2/3) de sus miembros presentes. Diseñar y fijar la política general del Ministerio Público Fiscal de la Nación y, en particular, la política de persecución penal que permita el ejercicio eficaz de la acción penal pública. Artículos 11 y 12 de la Ley 27.148 Orgánica del Ministerio Público Fiscal.
- 170 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 13.9.
- 171 *Ibíd.*, artículo 32.
- 172 *Ibíd.*, artículo 33.
- 173 *Ibíd.*, artículo 16.
- 174 Asociación por los Derechos Civiles, “Quién vigila a los que vigilan”, p. 15.
- 175 *Ibíd.*, p. 14.

- 176 Di Santi, Matías, “Marcelo Fuentes: ‘Las funciones de la Comisión están claras y su trabajo también’”, *Chequeado.com*, 3 de febrero de 2015. Disponible en: <http://chequeado.com/ultimas-noticias/marcelo-fuentes-las-funciones-de-la-comision-estan-claras-y-su-trabajo-tambien>
- 177 Ver página web de la Comisión Bicameral Permanente de Fiscalización de los Organismos y Actividades de Inteligencia -Ley 25.520. Disponible en: <http://www.senado.gov.ar/parlamentario/comisiones/proyectos/104>
- 178 “Cuestionan a la Comisión Bicameral de Inteligencia”, *La Nación*, 25 de febrero de 2014. Disponible en: <http://www.lanacion.com.ar/1667003-cuestionan-a-la-comision-bicameral-de-inteligencia>
- 179 Iniciativa Ciudadana para el Control del Sistema de Inteligencia.
- 180 Sued, Gabriel, “Se reúne la bicameral de Inteligencia”, *La Nación*, 3 de febrero de 2015. Disponible en: <http://www.lanacion.com.ar/1765255-se-reune-la-bicameral-de-inteligencia> y “A puertas cerradas y con la presencia de Parrilli, la bicameral de fiscalización de organismos de inteligencia analiza el proyecto oficial”, *Télam*, 5 de febrero de 2015. Disponible en: <http://www.telam.com.ar/notas/201502/94130-proyecto-sistema-de-inteligencia-bicameral-fiscalizacion.html>
- 181 “Espían y roban correos electrónicos de un juez y de un periodista de Clarín”, *Clarín*, 11 de mayo de 2006 y Sued, Gabriel, “Espían e-mails de políticos y periodistas”, *La Nación*, 23 de mayo de 2006. Disponible en: <http://www.lanacion.com.ar/808286-espian-e-mails-de-politicos-y-periodistas>
- 182 Palazzi, Pablo, *Los delitos informáticos en el Código Penal. Análisis de la ley No. 26.388*, Abeledo Perrot, 2012, pp. 20-22.
- 183 Véase también, Smink, Veronica, “Procesan al alcalde de Buenos Aires por caso de espionaje”, *BBC Mundo*, disponible en: [http://www.bbc.com/mundo/america\\_latina/2010/05/100514\\_2318\\_macri\\_proceso\\_buenos\\_aires\\_jg.shtml](http://www.bbc.com/mundo/america_latina/2010/05/100514_2318_macri_proceso_buenos_aires_jg.shtml) y Hauser, Irina y Kollmann, Raúl, “El día que Macri quedó Procesado”, *Página 12*, 15 de mayo de 2010. Disponible en: <http://www.pagina12.com.ar/diario/elpais/1-145731-2010-05-15.html>
- 184 “Escuchas ilegales: la Cámara Federal confirmó el procesamiento de Macri”, *Perfil*, 15/07/2010. Disponible en: <http://www.perfil.com/politica/Escuchas-ilegales-la-Camara-Federal-confirmo-el-procesamiento-de-Macri-20100715-0019.html>
- 185 Véase, “Una denuncia contra la Gendarmería”, *Página 12*, 22 de noviembre de 2011. Disponible en: <http://www.pagina12.com.ar/diario/elpais/1-181754-2011-11-22.html>; Thieberger, Mariano, “Proyecto X: Cómo espionó la Gendarmería a más de mil organizaciones”, *Clarín*, 10 de octubre de 2013. Disponible en: [http://www.clarin.com/zona/espio-Gendarmeria-mil-organizaciones\\_o\\_88012088.html](http://www.clarin.com/zona/espio-Gendarmeria-mil-organizaciones_o_88012088.html); Riera, Ariel y Tarricone, Manuel, “CFK: “Quisieron montar (...) que había una suerte de espionaje de la Gendarmería, Proyecto X, inexistente”. Disponible en: <https://eff.org/r.ktax>; “Un escándalo que reveló la cara oculta de la política de seguridad”, *Clarín*, 10 de octubre de 2013. Disponible en: [http://www.clarin.com/zona/escandalo-revelo-oculta-politica-seguridad\\_o\\_88012093.html](http://www.clarin.com/zona/escandalo-revelo-oculta-politica-seguridad_o_88012093.html)
- 186 Se puede tomar dimensión del alcance de Proyecto X viendo la lista completa de las organizaciones en todo el país que fueron objeto de las actividades de inteligencia de la Gendarmería Nacional. Véase, Savoia, Claudio, *supra* nota 92, p. 341-383.
- 187 “No admitimos espionaje”, *Página 12*, 18 de febrero de 2012. Disponible en: <http://www.pagina12.com.ar/diario/elpais/1-187848-2012-02-18.html>
- 188 Ley de datos personales, artículo 4.
- 189 *Ibíd.*, artículo 7.

- 190 *Ibíd.*, artículo 2.
- 191 Entrevista a Beatriz Busaniche de la Fundación Vía Libre, “Acá se vigila a quienes interpelan al poder”, *Perfil*, 02 de enero de 2015. Disponible en: <http://www.perfil.com/elobservador/Aca-se-vigila-a-quienes-interpelan-al-poder-20150102-0062.html>, Santoro, Daniel, “El Gobierno compró equipos para espiar mails y llamados”, *Clarín*, 15 de noviembre de 2014. Disponible en: [http://www.clarin.com/politica/Organismos\\_de\\_inteligencia-vigilancia-SIDE-espionaje\\_o\\_1249075526.html](http://www.clarin.com/politica/Organismos_de_inteligencia-vigilancia-SIDE-espionaje_o_1249075526.html) y Savoia, Claudio, *supra* nota 92, p. 220.
- 192 “Hacking Team”, 8 de julio de 2015. Disponible en: <https://wikileaks.org/hackingteam/emails/emailid/4517>
- 193 Ver más en “Hallan muerto al fiscal Alberto Nisman en su departamento de Puerto Madero”, *La Nación*, 19 de enero de 2015. Disponible en: <http://www.lanacion.com.ar/1761270-hallan-muerto-al-fiscal-alberto-nisman-en-su-departamento-de-puerto-madero> y “AMIA Special Prosecutor Alberto Nisman found dead in his Puerto Madero home”, *Buenos Aires Herald*, 19 de enero de 2015. Disponible en: <http://www.buenosairesherald.com/article/179900/amia-special-prosecutor-alberto-nisman-found-dead-in-his-puerto-madero-home>
- 194 Marquis-Boire, Morgan, “Dentro de la campaña de spyware contra alborotadores argentinos” [*Inside the Spyware Campaign Against Argentine Troublemakers*], *The Intercept*, 21 de Abril del 2015. Disponible en: <https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/>
- 195 En este mismo sentido, los peritos locales afirmaron que el software encontrado “sólo tiene efecto en computadoras”. Ver más en: Hauser, Irina, “Una lupa sobre el celular y la notebook”, *Página 12*, 8 de junio de 2015. Disponible en: <http://www.pagina12.com.ar/diario/elpais/1-274433-2015-06-08.html> y “Peritos dictaminaron que el virus en el celular del fiscal no sirve para espiar”, *Perfil*, 26 de agosto de 2015. Disponible en: <https://eff.org/r.8rvv>
- 196 Véase, O'Donnell, Santiago, “Caso Nisman. Pruebas y sospechas”, *Revista Anfibia*. Disponible en: <http://www.revistaanfibia.com/ensayo/pruebas-y-sospechas/> y Budassi, Sonia y Fidanza, Andrés, “El rompecabezas Nisman”, *Revista Anfibia*. Disponible en: <http://www.revistaanfibia.com/cronica/el-rompecabezas-nisman/>
- 197 Véase, Smink, Verónica, “Por qué Argentina tiene un problema con sus servicios de inteligencia”, *BBC Mundo*, 27 enero 2015. Disponible en: [http://www.bbc.com/mundo/noticias/2015/01/150126\\_argentina\\_nisman\\_espias\\_vs](http://www.bbc.com/mundo/noticias/2015/01/150126_argentina_nisman_espias_vs) y “Macri reclamó que la muerte de Nisman sea 'un antes y un después’”, *Clarín*, 19 de enero de 2015. Disponible en: [http://www.clarin.com/politica/Macri-reclamo-muerte-Nisman-bisagra\\_o\\_1288071426.html](http://www.clarin.com/politica/Macri-reclamo-muerte-Nisman-bisagra_o_1288071426.html)
- 198 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 5 bis.
- 199 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 5.
- 200 *Ibíd.*, artículo 60, punto d.
- 201 *Ibíd.*, artículo 5, punto 2.
- 202 Secretaría de Comunicaciones, *supra* nota 62, artículo 8.
- 203 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 60, punto d.
- 204 Ley No. 25.891 de Servicios de Comunicaciones Móviles, *supra* nota 64, artículo 8.

- 205 *La Nación*, “Florencio Randazzo anunció un nuevo DNI, con chip inteligente”, 27 de junio de 2014. Disponible en: <http://www.lanacion.com.ar/1705106-florencio-randazzo-anuncio-un-nuevo-dni-con-un-chip-inteligente>.
- 206 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 18.
- 207 *Ibíd.*, Título VI, artículo 18.
- 208 Ley de Protección de los Datos Personales No. 25.326.
- 209 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 19.
- 210 Ley No. 27.078 Argentina Digital, *supra* nota 56, artículo 5.
- 211 Secretaría de Comunicaciones, *supra* nota 62, artículo 8.
- 212 Ley 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 16 sexies.
- 213 Véase, Secretaría de Comunicaciones, *supra* nota 62 y ley de servicios de comunicación móviles, *supra* nota 64.
- 214 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 20.
- 215 *Ibíd.*, artículo 16.
- 216 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 16 sexies.
- 217 *Ibíd.*, artículo 42.
- 218 *Ibíd.*, artículo 19.
- 219 *Ibíd.*, artículo 41.
- 220 Código Penal, artículo 155.
- 221 Ley No. 25.520 de Inteligencia Nacional, *supra* nota 19, artículo 42.
- 222 *Ibíd.*, artículo 43.
- 223 *Ibíd.*
- 224 Véase, Bertoni, Eduardo, “Ley de inteligencia, oportunidad perdida”, Bastión Digital, 19 de febrero de 2015. Disponible en: <http://ar.bastiondigital.com/notas/ley-de-inteligencia-oportunidad-perdida#sthash.Td5djgIU.dpuf>
- 225 Siri, Laura, *supra* nota 77, p. 3.
- 226 *Ibíd.*
- 227 Véase, Bertoni, Eduardo, “Ley de inteligencia, oportunidad perdida”, Bastión Digital, 19 de febrero de 2015. Disponible en: <http://ar.bastiondigital.com/notas/ley-de-inteligencia-oportunidad-perdida#sthash.Td5djgIU.dpuf>