# Intimidad y privacidad frente a la interceptación de las comunicaciones electrónicas

Flavia Baladán[1], Jimena Hernández Varela[2]

[1] Baladán, Flavia, Doctora en Derecho y Ciencias Sociales, Asesor jurídico de Agesic, Miembro del Centro de Jurisprudencia de Derecho y Tecnologías y Aspirante a Profesor Adscripto del Centro de Derecho Informático de la UDELAR
Montevideo, Uruguay

[2] Hernández Varela, Jimena, Doctora en Derecho y Ciencias Sociales, Asesor jurídico de Agesic, Miembro del Centro de Jurisprudencia de Derecho y Tecnologías y Aspirante a Profesor Adscripto del Centro de Derecho Informático de la UDELAR
Montevideo, Uruguay

**Resumen.** Las tecnologías de la información constituyen herramientas que han producido grandes cambios en nuestra vida, siendo un elemento fundamental para la interacción y la comunicación entre las personas. Pero sin duda, su utilización como elemento de prueba no resulta exento de polémicas dado que, puede producir una colisión entre el fin perseguido y los derechos de las personas. La utilización de la vigilancia electrónica es un ejemplo claro en virtud de la intromisión que estas técnicas significan para la privacidad de las personas. Por ello, debemos analizar los elementos que permiten un equilibrio entre la privacidad y la utilización de herramientas de interceptación de las comunicaciones que se basan en la recolección de información de carácter privado con la finalidad de investigación y persecución de delitos. La utilización legitima de estas herramientas parece tener su clave en el hecho de estar inmersas en las garantías de los procesos judiciales y las resoluciones judiciales fundadas.

## 1. Introducción

Las tecnologías modernas en cuanto a la imagen, el sonido y la informática han significado cambios importantes en nuestras vidas, modificando la forma en que nos relacionamos y nos comunicamos.

El teléfono ha sido sin lugar a dudas una de las invenciones más trascendentes en la evolución de las comunicaciones, seguido por la creación del teléfono móvil. El celular o teléfono móvil constituyó un cambio de paradigma en la forma en que nos comunicamos, llegando a ser el principal instrumento. El primer aparato móvil fue desarrollado en el año 1973 por Martin Cooper en Nueva York, desde donde se realizó la primera llamada desde el DynaTAC 8000X creado por Motorola y presentado oficialmente en el año 1984. El teléfono pesaba cerca de 800 gramos y tenía un tamaño de 3,3 x 4,4 x 8,8 centímetros y un costo de $ 3.395 dólares americanos y su batería duraba una hora de comunicación.

Desde ese punto de partida, se produjo una gran expansión que hace que actualmente no podamos poner en duda la trascendencia que tiene en nuestra vida cotidiana la utilización de estos dispositivos.

Algunos estudios que se han realizado por la Agencia de Marketing y comunicación online 2.0, We are social, indican que la mitad de la población mundial es usuario de un teléfono móvil, generándose más de 750.000 nuevos usuarios móviles por día, o 9 por segundo.

Desde el punto de vista jurídico, la utilización de dispositivos móviles puede acaecer diversas consecuencias en su mayoría asociadas a la intimidad y privacidad de los usuarios. Pero también debemos mencionar sus virtudes cómo instrumento que permite acceder, en situaciones limitadas y legalmente establecidas, a su contenido con el objetivo de la represión del delito para la protección de los derechos de las personas.

En el presente trabajo nos proponemos analizar la forma en que las comunicaciones telefónicas son utilizadas como medios de prueba en los procesos judiciales. El análisis del alcance de las interceptaciones telefónicas, sus variantes y los diversos aspectos relacionados, parece ser un tema fundamental para que ésta opere dentro de los límites establecidos, teniendo en cuenta que en ella se produce una limitación de derechos, en pro de la defensa de otros.

## 2. Regulación de la intimidad y la intervención en las comunicaciones

La doctrina a nivel internacional es conteste en sostener la importancia de las herramientas de vigilancia electrónica e interceptación de comunicaciones como elementos fundamentales para la construcción de la prueba en el proceso penal.

Asimismo, también lo es en cuanto a la injerencia que implica en la vida de las persona dado que la interceptación de las comunicaciones telefónicas o de la correspondencia privada, puede exponer aspectos de la vida íntima de una persona. Por ello, debe verificarse una proporcionalidad entre los derechos lesionados y la medida adoptada.

### 2.1. Ponderación de Derechos en juego

Cuando nos proponemos hablar de los derechos que pueden resultar afectados cuando se utilizan métodos de vigilancia electrónica o interceptación de las comunicaciones electrónicas de las personas, parece oportuno referir a algunos conceptos aportados por Robert Alexy1 cuando en su Teoría de los derechos fundamentales refiere a la colisión de principios indicando que "*Cuando dos principios entran en colisión —tal como es el caso cuando según un principio algo está prohibido y, según otro principio, está permitido— uno de los dos principios tiene que ceder ante el otro. Pero, esto no significa declarar inválido al principio desplazado ni que en el principio desplazado haya que introducir una cláusula de excepción. Más bien lo que su-*

*cede es que, bajo ciertas circunstancias uno de los principios precede al otro. Bajo otras circunstancias, la cuestión de la precedencia puede ser solucionada de manera inversa*." Asimismo, enseña que "*cuanto mayor es el grado de la no satisfacción o de afectación de un principio, tanto mayor tiene que ser la importancia de la satisfacción del otro*".

Esta regla es la que el maestro denomina "*ley de la ponderación"* de acuerdo con la cual "*la medida permitida de no satisfacción o de afectación de uno de los principios depende del grado de importancia de la satisfacción del otro*".

No hay lugar a dudas de que la interceptación de las comunicaciones electrónicas produce una intromisión en la vida privada de las personas. Se produce una afectación a la intimidad que resulta de la ponderación realizada en pro de la defensa de otros derechos, y de acuerdo a una finalidad específica de represión del delito y bajo los principios de proporcionalidad y mínima intervención.

**2.2 Derecho a la intimidad y derecho a la privacidad**

La protección de la intimidad y la privacidad de las personas han sido reconocidas en numerosos textos normativos de carácter internacional, regional y nacional como derechos personalísimos, inherentes a la persona humana.

Únicamente a los efectos de remarcar la influencia de las tecnologías y los nuevos desafíos que estas presentan para los derechos y su protección, nos parece importante recordar lo que nos enseña el Profesor Carlos Delpiazzo[2] cuando indica que la globalización de la información privada ha exorbitado el concepto clásico de intimidad, abriendo cauce a su distinción con la privacidad o privacy, concebida como más amplia por aludir a datos no íntimos pero que la persona no quiere que sean difundidos. Recuerda en esta línea la antigua Ley española de protección de datos Nº 5/1992 la cual indica en su exposición de motivos que la intimidad "*protege la esfera en la que se desarrollan las facetas más singularmente reservadas de la vida de la persona"*, mientras que la privacidad "*constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado*".

Los conceptos intimidad, privacidad y protección de datos personales tienen como base la información sobre una persona. En el mundo actual este concepto se encuentra vinculada a la posibilidad de realizar su tratamiento. Y es de destacar que en el contexto existente el tratamiento va a ser mayoritariamente automático.

En este marco surge la protección de los datos personales como un tercer nivel de protección. Es decir, en un primer nivel se protege la intimidad de la persona, en un segundo nivel se resguarda un rango más amplio de datos lo que se denomina privacidad y en un tercer nivel, se protege todo tratamiento de datos personales, esto es, surge el derecho a la protección de los datos personales. Éste último es entendido

como el amparo de las personas contra la posible utilización por terceros no autorizados de sus datos personales susceptibles de tratamiento automatizado.

**2.2.1 Instrumentos internacionales aplicables**

A nivel internacional, se ha reconocido el derecho a la protección de la vida privada y de la correspondencia, así como la defensa frente a las intromisiones arbitrarias a dicha vida.

La protección de la vida privada frente al Estado parece tener una doble dimensión abarcando el derecho a la no injerencia y a la no divulgación de la información privada que éste puede poseer respecto a las personas.

Este derecho aparece reconocido en dos de los principales tratados internacionales en materia de Derechos Humanos, que constituyeron el reconocimiento de la persona humana como sujeto de Derecho Internacional, además de su importancia como instrumentos atípicos por sus disposiciones de carácter obligatorio para los Estados.

De acuerdo a su aparición cronológica cabe destacar en primer lugar la Declaración Americana de los Derechos y Deberes del Hombre, aprobada en el mes de abril de 1948, que dispone en el capítulo I, artículo V, que "*Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar*"

Posteriormente, la Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948, establece en el artículo 12 que "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*".

También se debe tener presente el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, de 1966, que indica que "*Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"* y complementa diciendo que *"Toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques*".

Si miramos Europa debemos comenzar por mencionar el Convenio para la protección de los derechos humanos y de las libertades fundamentales, de 4 de noviembre de 1950, que en su artículo 8° regula el derecho al respecto a la vida privada y familiar, al domicilio y a la correspondencia. En este texto normativo también se expresa que no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho salvo que esté prevista en una Ley y constituya una medida democrática, y sea necesaria para, entre otras cosas, la seguridad nacional, la seguridad pública, la defensa del orden y la prevención de las infracciones penales.

Con similar redacción, la Carta de Derechos Fundamentales de la Unión Europea, de 7 de diciembre del año 2000, en su artículo 7° establece que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. A ello se agrega el artículo 8° que regula el derecho a la protección de los datos de carácter personal de las personas indicando expresamente que su tratamiento sólo puede realizarse con el consentimiento de la persona o en virtud de un fundamento provisto por la Ley.

También merece especial destaque la existencia de lo que se ha denominado el Marco regulador de las comunicaciones electrónicas. Este marco está compuesto por la Directiva 2002/20/CE o directiva de autorización, la Directiva 2002/19/ CE llamada directiva de acceso, la Directiva 2002/22/CE o directiva de servicio universal, la Directiva 2002/58/CE o directiva sobre la privacidad y las comunicaciones electrónicas, el Reglamento N° 1211/2009 que establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), y el Reglamento N° 531/2012, relativo a la itinerancia en las redes públicas.

De todas estas normas, cabe hacer especial hincapié en la Directiva sobre la privacidad y las comunicaciones electrónicas que protege la información que se intercambia a través de servicios públicos de comunicaciones electrónicas como internet y la telefonía móvil y fija, así como de sus redes de apoyo. Estos servicios y redes exigen normas y salvaguardias específicas para garantizar el derecho de los usuarios a la intimidad y la confidencialidad. La Directiva establece que los países de la Unión Europea deben garantizar la confidencialidad de las comunicaciones realizadas a través de las redes públicas. Deben prohibir que se escuchen, intercepten, almacenen o que se sometan a cualquier tipo de vigilancia o interceptación las comunicaciones y datos de tráfico sin el consentimiento de los usuarios, salvo si la persona está autorizada legalmente a hacerlo y respeta unos requisitos específicos. Asimismo, se debe garantizar que únicamente se permita el almacenamiento de información o el acceso a la información almacenada en el equipo personal de un abonado si éste ha recibido una información clara y completa, como mínimo sobre la finalidad, y que además se le otorgue el derecho a rechazarlo.

Por su parte, la protección de datos personales se encuentra contemplada en la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. Esta norma indica que los Estados miembros podrán adoptar medidas legales para limitar el derecho a la protección de datos personales cuando ésta se base, entre otros casos, en la salvaguarda de la seguridad del Estado, la defensa, la seguridad pública, o la prevención, investigación, detección y represión de infracciones penales.

Es interesante destacar que esta normativa ha sido revisada, y se encuentra pendiente de entrar en vigor, el nuevo Reglamento de Protección de Datos que empezará a regir a partir de mayo del año 2018. De esta norma cabe destacar la revisión que se hizo del tratamiento de los datos en materia de cooperación policial. En este sentido *"El nuevo paquete de protección de datos también incluye una directiva sobre transmisión de datos para cuestiones judiciales y policiales. Se aplicará al intercambio de datos transfronterizos dentro de la UE y establecerá*

*estándares mínimos para el tratamiento de datos en cada país. La intención es proteger a las personas implicadas en investigaciones policiales o procesos judiciales, sea como víctimas, acusados o testigos, mediante la clarificación de sus derechos y el establecimiento de límites en la transmisión de datos para prevención, investigación, detección y enjuiciamiento de delitos o la imposición de penas. Se han incluido salvaguardas para evitar riesgos para la seguridad pública, al tiempo que se facilita una cooperación más rápida y efectiva entre las autoridades policiales y judiciales*". [3]

Más allá de la existencia de una regulación a nivel europeo en términos generales, cabe hacer especial referencia a la ley de vigilancia aprobada en Francia en el año 2015 que sigue los lineamientos de la Patriot Act de Estados Unidos. Esta norma establece que las autoridades pueden vigilar las comunicaciones electrónicas de cualquier persona vinculada a una investigación terrorista o sospechosa de ilegalidad, sin la necesidad de previa autorización judicial. También obliga a los proveedores de servicios de Internet y las operadoras telefónicas a ceder los datos de los clientes si así lo requieren las agencias de inteligencia. Además, pueden monitorear el tráfico de internet buscando patrones de conducta bajo palabras clave de quien las escribe, sitios de consulta o personas con las que se contactan. A ello se agrega que está autorizado colocar dispositivos de grabación en las viviendas de los sospechosos.

Por último, cabe mencionar la existencia de una iniciativa ciudadana presentada ante la Comisión Europea en el año 2015 que tiene por objetivo reforzar los aspectos legales de la confidencialidad de las comunicaciones entre particulares, en especial entre el abogado y su cliente.[4]

También es interesante destacar que en Estados Unidos, encontramos regulación de la vigilancia electrónica tanto en la Constitución Federal como a nivel de los Estados a través de las leyes federales. La Cuarta Enmienda de la Constitución Americana prohíbe que el gobierno incurra en allanamientos y decomisos arbitrarios. Se requiere una orden de allanamiento antes de registrar un lugar, y ello aplica a los dispositivos electrónicos y a otras formas de almacenamiento de datos en forma digital. Por su parte, la ley de Privacidad de las Comunicaciones Electrónicas (Electronic Communications Privacy Act) regula el acceso policial a diferentes formatos de datos electrónicos. El Título I es la Ley de Escuchas (Wiretap Act), que regula cómo el gobierno puede interceptar el contenido de comunicaciones, por ejemplo las telefónicas. El Título II es la Ley de Almacenamiento de las Comunicaciones (Stored Communications Act), referida al acceso al contenido de comunicaciones electrónicas como correos electrónicos, tweets, mensajes de texto, etc. Se debe puntualizar que la mayoría de los estados han adoptado estas disposiciones.

### 2.2.2 Instrumentos nacionales aplicables

En Uruguay contamos con un marco normativo que regula las comunicaciones y establece determinadas condiciones y garantías a su respecto.

En primer lugar, debemos mencionar el artículo 28 de la Constitución de la República, ubicado dentro del Capítulo de Deberes, derechos y garantías, que indica que la correspondencia de cualquier especie es inviolable y no puede realizarse su registro, examen o interceptación, excepto las leyes que se establecen por razones de interés general.

Conforme con lo dispuesto en esta norma, solamente procede la interceptación de comunicaciones cuando sea soportada por una norma habilitante de rango legal. Dicho de otra forma, al encontrarse esta disposición dentro del capítulo que regula los derechos, deberes y garantías, será necesaria la existencia de una norma de rango legal, basada en un interés general, la que permita la realización de cualquier tipo de interceptación.

A ello, se debe agregar que nuestro país cuenta con un régimen legal para tutelar la privacidad de las personas. Es así que la Ley N° 18.331, de 11 de agosto de 2008, establece que el derecho a la protección de datos personales es un derecho humano que se encuentra incluido dentro del artículo 72 de nuestra Constitución. Esta norma refiere a que "*la enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno*".

El derecho a la privacidad implica que nadie puede ser objeto de injerencias arbitrarias o ilícitas en su vida privada. En este marco, debemos entender que la interceptación de las comunicaciones debe realizarse también conforme con las condiciones que establece esta normativa.

En este aspecto, es importante resaltar que dato personal es toda aquella información que identifica o puede identificar a una persona, incluso la imagen y la voz. En el marco de la interceptación de comunicaciones electrónicas existe acceso y conocimiento por parte de la Entidad que realiza la interceptación, de una gran cantidad de datos de carácter personal correspondientes a todas las personas que puedan estar involucradas en la comunicación. Ello incluye a los sujetos indagados y a todas las personas que establezcan contacto con él.

En este sentido, cabe hacer especial referencia a lo que estipula el artículo 25 de la Ley que se refiere a las bases de datos correspondientes a las Fuerzas Armadas, Organismos Policiales o de Inteligencia. Es de especial interés remarcar que el artículo establece que el tratamiento de datos personales con fines de defensa nacional o seguridad pública, por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública, o la represión de delitos. En este caso, los datos personales registrados con los fines mencionados se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Por tanto, y conforme con lo que venimos expresando, solamente podrán tratarse datos personales sin consentimiento de sus titulares, en el marco de una vigilancia electrónica o una interceptación de comunicaciones electrónicas, y cuando ésta tenga por finalidad la defensa nacional, la seguridad pública o la represión de delitos. Como vemos, se trata de otros bienes jurídicos tutelados también a nivel constitucional y legal. En este caso entonces estamos en presencia de una ponderación de derechos, donde la protección de datos personales cede frente a la existencia de intereses superiores a proteger.

En interesante sumar a este estudio la perspectiva del derecho penal nacional. Dentro de los delitos previstos en el Código Penal Uruguayo se encuentran aquellos que protegen como bien jurídico la inviolabilidad del secreto. A efectos de tutelar este bien jurídico encontramos dos figuras penales que hacen referencia a la inviolabilidad y a la revelación de las comunicaciones telefónicas, telegráficas o epistolares.

Por un lado, el delito de interceptación de noticia, telegráfica o telefónica se configura cuando una persona intercepta una comunicación telefónica, la impide o la interrumpe utilizando para ello artificios. En este caso la normativa prevé una sanción de 20 a 400 Unidades Reajustables.

Por otro lado, se prevé el delito de revelación de secreto de la correspondencia y de la comunicación epistolar, telegráfica o telefónica. En este caso, la conducta ya no consiste en interceptar o interrumpir una comunicación sino que pena a aquella persona que sin justa causa comunica a los demás lo que ha llegado a su conocimiento, o publica el contenido de una comunicación telefónica que le estuviere dirigida y que por su naturaleza debiera ser secreta. En este caso la sanción es de 20 a 200 Unidades Reajustables.

## 3. Legitimación para la intervención de comunicaciones electrónicas en Uruguay

En este apartado se pretende relevar todos los requerimientos que el ordenamiento jurídico de nuestro país requiere para que sea considerada lícita la interceptación de comunicaciones electrónicas.

A esos efectos, y como hemos mencionado up supra, se debe empezar por señalar que el artículo 28 de nuestra Constitución Nacional indica que "*los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier especie son inviolables y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieran por razones de interés general*".

Es así que esta norma merece dos consideraciones. En primer lugar, la interceptación de las comunicaciones electrónicas ingresa dentro del amparo de la referida norma dado que refiere y abarca las comunicaciones de cualquier especie. En segundo lugar, que el artículo 212 de nuestro Código de Proceso Penal, que fue parcialmente modificado por el artículo 5° de la Ley N° 18.494, de 5 de junio de 2009, establece

cuándo se puede disponer y realizar la vigilancia electrónica o la interceptación de comunicaciones, cumpliendo con lo dispuesto en la norma constitucional.

En cuanto al interés general requerido para limitar lo dispuesto en la Carta, se requiere que la interceptación de las comunicaciones electrónicas sea solicitada por el Ministerio Público y Fiscal, y mandatada por un juez competente que se encuentre a cargo de la investigación que da lugar a tal requerimiento.

La referida resolución judicial deberá contener determinados requisitos para ser considerada lícita y suficiente. En este sentido, en Derecho comparado se han identificado los límites en los cuales se puede realizar una vigilancia electrónica. Es así que se considera necesario que se dé en el marco de un delito debiendo ser vulnerado un bien jurídico mayor. Debe ser por un período de tiempo determinado, pudiendo ser extendido mediante solicitud del Ministerio Público y se necesita una resolución fundada del juez. Es necesario que también se limite el lugar de la vigilancia electrónica. Se solicita además determinar quienes intervienen en la vigilancia. Además, se deben avalar todas las garantías del debido proceso. Por último, pero esencial para realizar la vigilancia, es que ésta tenga como finalidad descubrir o comprobar algún hecho o circunstancia del ilícito investigado. [5]

En este tema es importante referirse al principio de publicidad del proceso penal. En nuestro ordenamiento jurídico este principio es recogido por el artículo 113 del Código del Proceso Penal, aunque sea limitado para los partícipes del proceso desde lo que se denomina etapa de presumario. Salvo resolución fundada del Juez basada en la posible frustración de las pruebas a diligenciar. En este sentido, como la vigilancia electrónica se trata de una excepción, debe ser utilizada en forma restrictiva.

También es de destacar que el artículo 5° de la Ley 18.494, de 5 de junio de 2009, regula la adopción de medidas de vigilancia electrónica. En este sentido dentro del concepto de vigilancia electrónica quedan incorporadas la interceptación de la correspondencia, las comunicaciones telefónicas, las comunicaciones electrónicas de cualquier tipo, o la utilización de micrófonos, cámaras, imágenes satelitales, etc. "*Es que la norma prevé que se puedan utilizar "todos los medios tecnológicos disponibles", con lo cual la herramienta no permanece pétrea ante los cambios incesantes*".

Por último cabe considerar que en la utilización de la técnica en cuestión pueden existir diferencias en la hipótesis de que una parte tenga conocimiento de que se está procediendo con algún tipo de vigilancia electrónica. Cuando esto suceda puede ser que ese sujeto sea al mismo tiempo un colaborador, un agente encubierto u otra persona que encarte o no en algunas de las categorías reguladas en la referida Ley.

### 3.1. El "Guardián"

En este apartado se pretende referir algunas cuestiones de relevancia que se han suscitado en Uruguay en relación al tema. Específicamente, respecto a la adquisición de un sistema de vigilancia electrónica denominado "El Guardián".

Se trata de un sistema informático adquirido por el Ministerio del Interior que permite unificar las escuchas telefónicas que realizan 22 dependencias del referido Ministerio, y acceder de manera simultánea a 800 celulares y 200 teléfonos fijos, correos electrónicos y redes sociales. [6]

En el marco del funcionamiento de este nuevo Sistema se suscribió, con fecha 1° de diciembre de 2016 un Protocolo de Actuación para Interceptaciones Legales de Comunicaciones[7], entre el Ministerio del Interior, la Fiscalía General de la Nación y la Suprema Corte de Justicia. Este documento constituye un Memorando de Entendimiento donde se determina el proceso de tramitación de los requerimientos de información e interceptación legal de comunicaciones. Tiene como finalidad dotar de transparencia al flujo de solicitudes, las decisiones de los Magistrados con competencia legal y las respuestas de las empresas operadoras de telecomunicaciones.

Las partes asumen en este documento el compromiso de garantizar la reserva de todas las actuaciones tendientes al sistema de interceptación de comunicaciones. El Sistema cuenta con un Sistema Administrativo de Interceptaciones Legales, denominado SAIL, para dar soporte administrativo a las solicitudes de interceptación, decisiones y respuestas.

Asimismo, regula el proceso de tramitación de los requerimientos de información e interceptaciones legales. En el marco de una investigación criminal, y cuando la autoridad considere indispensable la ejecución de vigilancias electrónicas, debe emitir comunicación al Juez Penal competente que es quien, previo pronunciamiento del Ministerio Público, decide sobre la solicitud, emitiendo o no la orden a la empresa de telecomunicaciones que corresponda.

La adquisición de este Sistema de vigilancia no resultó exenta de debate público. Es así, que fue objeto de una acción de acceso a la información pública por parte de una ONG nacional. El Tribunal de Apelaciones en lo Civil de 5º Turno Nº SEF 0004-000051/2015 de fecha 21 de abril de 2015 confirma la sentencia de primera instancia que desestimó la acción de acceso a la información pública presentada contra el Ministerio del Interior solicitando información sobre el sistema de vigilancia e interceptación de telecomunicaciones denominado el Guardián. El agravio indica que se lesiono el derecho de acceso y que debía entregarse la información por no haberse concreado razones de secreto, reserva o confidencialidad. El Tribunal, por su parte, entiende que no se vulnera el derecho de acceso a la información pública, afirmando que se trata de un derecho que no tiene carácter irrestricto y absoluto, pues la protección de otros derechos consagrados constitucionalmente determinan que puedan existir excepciones legales al deber de brindar la información. Entiende que le asiste razón al recurrente en cuanto a que operó el silencio positivo, por no haber resuelto la petición de acceso en el plazo legal establecido.

Respecto a la información objeto de la solicitud el Tribunal, remarca que el secreto de la operación de adquisición del "guardián", declarada secreta por el Tribunal de Cuentas, radica no sólo en la compra en sí misma, sino que también alcanza a las características técnicas del producto. Ello, por razones de seguridad y protección

de los derechos de todos los habitantes mediante la prevención y represión de ilícitos. En definitiva, el Tribunal entiende que la información solicitada queda legalmente exceptuada como secreto de acuerdo con lo establecido por el artículo 8º de la Ley Nº 18.381.

### 3.2. Algunos fallos jurisprudenciales de interés

La jurisprudencia en Uruguay no ha sido indiferente a la utilización de herramientas de vigilancia electrónica y de interceptación de las comunicaciones electrónicas como medio para la investigación y procesamiento de ilícitos penales.

Es así que ya en el año 2010 el Tribunal de Apelaciones en lo Penal de 3° Turno dictaba la sentencia N° 193 de 12 de abril de ese año. En el caso se confirma un auto de procesamiento por homicidio por el cual la vinculación del encausado se pudo establecer por mensajes de texto y estudio del tráfico de las comunicaciones del celular de la víctima. De la sentencia surge que del estudio del tráfico de las comunicaciones se desprende que desde la fecha de la desaparición de la víctima el aparato estuvo en poder del autor del delito, el cual no dio ninguna explicación razonable a su respecto, siendo por tanto parte de la prueba que se tomó para vincular al autor con la víctima.[8]

También merece especial destaque la sentencia N° 259 de 23 de diciembre de 2011 dictada por el Juzgado Letrado de Primera Instancia en lo Penal de 1° Turno. En este caso se condena a una persona por un delito de simulación de delito, el cual es probado porque se ubica a la victima a través del rastreo de su celular. El aspecto de interés de la sentencia radica en que la investigación policial se basó en la localización de la ubicación del teléfono desde el cual se enviaban los mensajes de texto a partir del tráfico de llamadas y mensajes enviados. Con ello se logra probar la falsedad de la denuncia y de toda la historia elaborada y se condena a la supuesta víctima por el referido delito.[9]

Otra sentencia de interés resulta la emitida en un proceso judicial que finalizó en el año 2014 donde se utilizó un sistema de vigilancia electrónica para identificar y condenar a los involucrados. Se trata de un caso de tráfico ilícito de estupefacientes donde el resultado de la utilización de este método fue prueba fundamental para procesar a los autores del referido delito. El proceso tuvo dos instancias. La primera instancia fue la sentencia N° 12 de 4 de junio de 2013 dictada por la Jueza Letrada de Primera Instancia de Crimen Organizado de 2° Turno. La segunda instancia fue la sentencia dictada por el Tribunal de Apelaciones en lo Penal de 2° Turno donde se confirma lo dictaminado en la primera instancia.[10] La sentencia es de destaque en virtud de las consideraciones que realiza en Tribunal respecto a la utilización legitima y proporcionada de las herramientas de vigilancia electrónica, en el caso, las interceptaciones telefónicas.

## 4. Reflexiones finales

La interceptación de las comunicaciones forma parte de nuestra vida actual constituyendo uno de los cambios que ha aparejado la sociedad de la información en la cual nos encontramos inmersos. En este sentido, las herramientas tecnológicas permiten una mayor injerencia en nuestra intimidad y vida privada como no se había visto antes.

Ante esta nueva realidad, el derecho no debe permanecer indiferente. Para ello contamos con un extenso marco de protección de la intimidad y la privacidad de las personas, así como sobre la regulación de las comunicaciones en sus diversos formatos que resulta plenamente aplicable.

Desde el punto de vista jurídico, y para encuadrar el tema, es importante distinguir entre el derecho a la intimidad como la parte más reservada de la persona, la privacidad como aquellos datos que hacen posible su identificación y forman parte de su ser en un sentido más amplio que el anterior, y la protección de los datos personales como el derecho a resguardar toda información referida a ella.

En este marco, la interceptación de las comunicaciones implica el acceso a una gran cantidad de datos personales requiriendo limitar y garantizar dicha posibilidad. Es así que surge la necesidad de contar con una normativa que explicite los contenidos que debe poseer para ser considerada lícita.

Respecto a éste último punto, se pueden mencionar, sin perjuicio de la existencia de otros, que la posible normativa debe contener disposiciones que regulen que la interceptación de las comunicaciones se dé en el marco de un delito debiendo ser vulnerado un bien jurídico mayor, debe ser por un período de tiempo, contar con una resolución judicial así como con la determinación de quienes intervienen en la vigilancia, y fundamentalmente avalar todas las garantías del debido proceso. Por último, pero esencial para realizar la vigilancia, es que ésta tenga como finalidad descubrir o comprobar algún hecho o circunstancia del ilícito investigado.

También aporta a ello la existencia de procesos judiciales eficientes y garantistas, el rol activo del Ministerio Público y Fiscal y las resoluciones judiciales fundadas. Es en el análisis de la jurisprudencia donde podemos evidenciar la importancia probatoria de la interceptación de las comunicaciones como elemento determinante para la investigación y procesamiento de los implicados en actividades ilícitas.

En este caso, como en todos en los que puede producirse una colisión entre derechos fundamentales, es vital el rol de los operadores del derecho a la hora de determinar y ponderar los diversos bienes jurídicos en juego con la finalidad de brindar las mayores garantías posibles para los derechos de las personas.

## Referencias

[1] Alexy, Robert. Teoría de los derechos fundamentales. Centro de Estudios Constitucionales. Madrid (1993) 89 y 161.

[2] Delpiazzo, Carlos y Viega, María José. Lecciones de Derecho Telemático. Tomo II. Fundación de Cultura Universitaria. Montevideo (2009) 57

[3] Información disponible en:
http://noticias.juridicas.com/actualidad/noticias/11018-aprobado-el-reglamento-europeo-de-proteccion-de-datos:-nuevas-reglas-adaptadas-a-la-era-digital/

[4] Información disponible en:
http://cnb.avocat.fr/Iniciativa-ciudadana-europea-sobre-la-vigilancia-electronica-masiva_a2258.html

[5] Información disponible en:
http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4523-proceso-penal-y-crimen-organizado:-particularidades-procesales-en-espana-y-en-uruguay-con-enfasis-en-la-problematica-probatoria/

[6] Información disponible en:
http://www.portaltnu.com.uy/video.php?vid=905

[7] Información disponible en:
http://www.poderjudicial.gub.uy/images/institucional/memorando_entendimiento_sail_interceptaciones_01-12-15.pdf

[8] Anuario de Derecho Informático. Tomo XI. Instituto de Derecho Informático. Fundación de Cultura Universitaria. Montevideo (2010) 281.

[9] Anuario de Derecho Informático. Tomo XIII. Instituto de Derecho Informático. Fundación de Cultura Universitaria. Montevideo (2012) 323.

[10] Información disponible en:
http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=577