# Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en Colombia

Por Juan Camilo Rivera y Katitza Rodríguez

Marzo 2016

ELECTRONIC FRONTIER FOUNDATION

Comisión Colombiana de Juristas

Fundación Karisma
www.karisma.org.co

Juan Camilo Rivera es abogado de la Universidad del Rosario (Bogotá), donde actualmente es profesor de Teoría del Derecho. Tiene una maestría en Derecho en la Universidad de los Andes (Bogotá). Trabajó durante varios años en la Comisión Colombiana de Juristas, realizando litigio estratégico en casos de derechos humanos, y actualmente es asesor en el Senado de la República de Colombia.

Katitza Rodríguez es la directora de derechos internacionales de la Electronic Frontier Foundation. Se concentra en la política comparativa de los asuntos de privacidad a nivel internacional, con especial énfasis en la aplicación de la ley, vigilancia gubernamental y el flujo transfronterizo de datos. Katitza posee el título de Licenciada en Derecho por la Universidad de Lima, Perú.

Informe preparado para la Electronic Frontier Foundation. Agradecemos la contribución sustantiva de los expertos colombianos en derechos humanos, Carolina Botero y Juan Diego Castañeda, ambos miembros de la Fundación Karisma, y Mateo Gomez, Comisión Colombiana de Juristas, Kim Carlson y David Bogado de EFF por la edición y formato.

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, una organización internacional sin fines de lucro que desde 1990 defiende la libertad de expresión y la privacidad en el entorno digital.

# Tablas de Contenido

# I.
# Introducción

En la actualidad, cada vez los Estados cuentan con mayores medios tecnológicos para vigilar las comunicaciones de las personas. Como lo señaló el Relator Especial de las Naciones Unidas para la libertad de expresión en su Reporte del año 2013, debido a los avances tecnológicos, ahora más que nunca los Estados cuentan con una mayor capacidad para realizar vigilancia simultánea, invasiva, focalizada y de larga escala.[1] Esto plantea un riesgo para distintos derechos reconocidos en las constituciones de los Estados y en tratados internacionales de derechos humanos ratificados por ellos. Entre estos derechos se encuentran la intimidad, ya que información privada puede ser consultada sin autorización del titular; la libertad de asociación, ya que puede conocerse lo que en ejercicio de este derecho un grupo de personas haga o discuta; la libertad de expresión, ya que el riesgo de que las comunicaciones sean vigiladas puede llevar a la autocensura o acarrear represión por parte de la autoridad, y el acceso a la información, ya que la información que es recolectada y almacenada a través de la vigilancia puede ser mantenida oculta y puede ser usada en un futuro.

Este avance de la vigilancia estatal de las comunicaciones no siempre ha ido a la par de una respuesta que busca proteger los derechos que ella amenaza.[2] Colombia no ha sido una excepción a esta tendencia. La legislación en materia de vigilancia de las comunicaciones es dispersa e incompleta. Esta se encuentra contenida en la Constitución, en múltiples leyes, decretos y reglamentos, a los que hay que añadir las disposiciones generales contenidas en tratados internacionales sobre derechos humanos. Además, en algunos casos la normativa ha sido dictada e implementada con posterioridad a la aplicación de ciertas técnicas y estrategias de vigilancia. Una muestra de ello es que los servicios de inteligencia en Colombia funcionaron durante casi sesenta años sin una regulación integral que demarcara sus funciones y sus límites,[3] hasta que dicha regulación se expidiera en 2013 a través de la ley 1621.[4]

La falta de un marco normativo claro e integral que regule y limite el avance del uso de las tecnologías de vigilancia por parte del Estado dificulta el control ciudadano de la manera como la vigilancia de las comunicaciones se desarrolla: subrepticiamente, impregnada de una cultura del secreto. Aún más grave, la ausencia de regulación en la materia puede constituir en sí misma un desconocimiento de la obligación que tienen los Estados que han suscrito tratados internacionales de derechos humanos de expedir legislación para hacer efectivos los derechos reconocidos en ellos.[5]

La regulación de la vigilancia estatal de las comunicaciones es un asunto de gran sensibilidad en el contexto colombiano, debido a los múltiples casos de repercusión pública ocurridos en años recientes con relación a este tema. Entre ellos se cuenta, por ejemplo, las arbitrariedades que de manera sistemática y generalizada fueron cometidas por los servicios de inteligencia entre los años 2003 y 2008, los cuales fueron utilizados para perseguir y vigilar periodistas, miembros de partidos de la oposición, defensores de derechos humanos, magistrados de las Altas Cortes, y, en general, personas que pudieran ser consideradas opositoras a las políticas gubernamentales.[6] Más recientemente, podría mencionarse la vigilancia de las comunicaciones que un grupo de inteligencia del Ejército realizó a los negociadores del Gobierno que participan en el proceso de paz con las Fuerzas Armadas revolucionarias de Colombia (FARC) que se adelanta en La Habana, Cuba[7] en una operación conocida como "Andrómeda", así como la filtración de información de inteligencia para propósitos electorales en las más recientes elecciones para Presidente de la República.[8]

En Diciembre del 2015, la prensa colombiana reveló que algunos periodistas colombianos vienen siendo objeto de vigilancia estatal de las comunicaciones, siendo la Policía Nacional uno de las instituciones en sospecha.[9] Dicha denuncia se enmarca en un contexto en el que se ha revelado que la Policía ha adquirido nuevos equipos de vigilancia masiva e intrusiva, tal como lo muestran dos informe publicados a mediados del 2015 por la ONG británica Privacy International[10] y las noticias en la prensa colombiana que revelan la preocupación del Fiscal General por el uso indiscriminado que se le podría dar a las nuevas tecnologías de interceptación en casos en que dicha "invasión de derechos fundamentales ni siquiera es necesaria en la lucha contra la criminalidad."[11] Con dicho contexto, el presente reporte pretende servir de herramienta en el propósito de evaluar la normativa y las prácticas vigentes, y con base en esa evaluación formular recomendaciones de mejora en la regulación y prácticas en materia de vigilancia estatal de las comunicaciones, de modo que sea en la mayor medida posible respetuosa de los derechos humanos. Para cumplir con dicho propósito general, el presente reporte aborda dos objetivos específicos.

El primero es identificar y exponer de manera ordenada la legislación vigente en Colombia que regula la vigilancia estatal de las comunicaciones, con el fin de facilitar la comprensión del marco jurídico de las actividades de vigilancia, los controles institucionales y las garantías de defensa con las que cuentan los particulares. Específicamente, el texto se centra en describir un aspecto de la vigilancia estatal de las comunicaciones, a saber: ¿de qué manera puede el Estado *acceder* a las comunicaciones de las personas? El énfasis en este tema se justifica por ser especialmente relevante estudiar la legislación interna en materia de protección de los derechos de las personas frente a la vigilancia estatal, con el fin de poner de presente los límites que las instituciones del Estado deben observar para poder llevarla a cabo.

El segundo objetivo específico de este reporte es exponer los estándares internacionales en materia de derechos humanos que sirven de límite a la vigilancia estatal de las comunicaciones y evaluar el nivel de cumplimiento de tales estándares por la normativa y las prácticas nacionales descritas. Estos estándares internacionales resultan aplicables a nivel interno en virtud del bloque de constitucionalidad, por lo que pueden ser invocados judicialmente para la protección de los derechos afectados por medidas de vigilancia estatal de las comunicaciones, así como para realizar labores de incidencia política en el delineamiento de la normativa y las prácticas de la autoridad en la materia.

El derecho internacional de los derechos humanos resulta de gran utilidad para estos propósitos en materia de vigilancia estatal de las comunicaciones, pues en los años recientes ha habido importantes pronunciamientos de organismos internacionales que han empezado a fijar criterios de interpretación y lineamientos para definir si un Estado está cumpliendo sus obligaciones en materia de derechos humanos en el marco de la vigilancia de las comunicaciones.

Debido a la complejidad del tema en sus aspectos técnicos y jurídicos utilizaremos las siguientes definiciones tal como las recoge los Principios Internacionales para la Aplicación de los Derechos Humanos en el Contexto de la Vigilancia de las Comunicaciones:[12]

- «Vigilancia de las Comunicaciones» en el entorno moderno comprende monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas;
- «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;
- "Información Protegida" es toda información que incluye, refleja, surge de, o se refiere a las comunicaciones de una persona y que no está fácilmente disponible y accesible para el público en general.

# II.
# Marco jurídico constitucional de la protección de los derechos fundamentales frente a la vigilancia estatal de las comunicaciones en Colombia

La vigilancia estatal de las comunicaciones puede entrar en tensión con distintos derechos fundamentales reconocidos por la Constitución y por distintos tratados internacionales de derechos humanos. Quizás el primero en el que se piensa cuando se habla de vigilancia de las comunicaciones es el derecho a la intimidad. Existen distintas normas, nacionales e internacionales, que regulan el contenido de este derecho, algunas de manera general, otras de manera más específica atendiendo a circunstancias concretas. De cualquier forma, como se mencionó brevemente en la introducción, la intimidad no es el único derecho que entra en tensión con la vigilancia estatal de las comunicaciones. Además de este, existen otros, como por ejemplo los derechos a la libertad de expresión y al acceso a la información, a la libertad de asociación y al debido proceso. Estos derechos también se encuentran regulados por disposiciones constitucionales generales y otras de tipo legal o reglamentario más concretas donde se define el alcance y el contenido de cada uno de ellos.

Para dar cuenta de este marco jurídico, es preciso hacer referencia a las principales disposiciones que regulan las comunicaciones de las personas. Con esta finalidad, en este reporte se hará un recuento de las principales disposiciones normativas que regulan la privacidad,[13] yendo de las disposiciones que tienen mayor jerarquía normativa a las de menor jerarquía. Por esto, se empezará mencionando las disposiciones de la Constitución Política sobre vigilancia de las comunicaciones, pues allí se establecen salvaguardas básicas que deben irradiar todas las regulaciones en materia de vigilancia estatal de las comunicaciones.

Como puede observarse, en el reporte se contrastarán las previsiones del derecho internacional sobre derechos humanos con lo dispuesto en la legislación nacional, lo cual se explica porque el ordenamiento jurídico colombiano reconoce al derecho internacional fuerza normativa. Esta fuerza normativa del derecho internacional no siempre es la misma, por lo que es preciso hacer algunas distinciones sobre la materia.

Por ello, se expondrá brevemente la doctrina de la Corte Constitucional sobre el bloque de constitucionalidad, enfocada específicamente a exponer la fuerza normativa que le ha otorgado a ciertos instrumentos internacionales de derechos humanos que tienen la misma naturaleza de algunos que, en los últimos años, se han ocupado de estudiar la aplicación de

los derechos humanos al contexto de la vigilancia de las comunicaciones.

## 2.1 Fuerza normativa en Colombia de tratados internacionales en materia de derechos humanos que pueden ser afectados por la vigilancia estatal de las comunicaciones

Distintos instrumentos internacionales y pronunciamientos de organismos internacionales hacen referencia a los derechos que pueden ser afectados por la vigilancia estatal de las comunicaciones. Incluirlos en el estudio del marco jurídico de la vigilancia de las comunicaciones en Colombia es necesario, ya que, por virtud de la propia Constitución Política, las normas internacionales tienen fuerza normativa en el ordenamiento jurídico interno. Según lo ha aclarado la jurisprudencia constitucional, en algunos casos esas disposiciones son vinculantes, mientras que en otros tienen fuerza interpretativa.

La fuerza normativa de algunas disposiciones de derecho internacional en el ordenamiento interno encuentra su fundamento en la Constitución misma. Esta establece distintas cláusulas expresas de remisión al derecho internacional, como lo hacen los artículos 53 (sobre convenios internacionales del trabajo), 93 (sobre tratados y normas de derechos humanos) y 214 (sobre el derecho internacional humanitario).

El artículo 93 establece la regla general en materia de los tratados y las normas de derechos humanos que tienen valor en el ordenamiento interno. De acuerdo con este artículo, existen tratados internacionales que tienen el mismo valor vinculante de la Constitución (aquellos ratificados por Colombia y que tratan sobre derechos humanos que no pueden ser suspendidos en estados de excepción), y otros que tienen valor interpretativo, en el sentido de que deben ser utilizados para determinar el alcance y el contenido de los derechos reconocidos en la Constitución.[14]

Con base en estas normas, y de manera consistente desde 1995,[15] la Corte Constitucional ha sostenido que algunos tratados de derechos humanos y de derecho internacional humanitario conforman, junto con el articulado de la Constitución, un *bloque de constitucionalidad*. Esto quiere decir que las normas que tienen fuerza constitucional no son sólo aquellas mencionadas en la Constitución, sino también otras, como las contenidas en algunos tratados internacionales de derechos humanos.[16]

Partiendo de este hecho, la Corte Constitucional ha dado fuerza normativa en el ordenamiento jurídico interno a otras fuentes de derecho internacional, como los pronunciamientos de organismos internacionales tales como la Comisión Interamericana de Derechos Humanos,[17] la Corte Interamericana de Derechos Humanos,[18] o los órganos de derechos humanos de Naciones Unidas.[19] También la Corte Constitucional le ha dado fuerza

normativa interna a instrumentos internacionales distintos a tratados internacionales, como a las declaraciones de principios surgidas de órganos de la Organización de Naciones Unidas.[20] En otras ocasiones, ha utilizado documentos de expertos sobre derechos humanos y ha sostenido que se trata de criterios hermenéuticos relevantes para la interpretación de las obligaciones sobre derechos humanos contraídas en virtud de la ratificación de tratados internacionales que hacen parte del bloque de constitucionalidad.[21]

Lo anterior es de gran importancia para la interpretación del marco jurídico en Colombia con relación a la vigilancia de las comunicaciones y su balance con el respeto de los derechos humanos. Debido a los avances tecnológicos en materia de la vigilancia de las comunicaciones, existen novedosos desafíos conceptuales para regular, los cuales en parte han sido abordados en los años recientes por organismos internacionales y por expertos que han trabajado para mostrar cómo el derecho internacional de los derechos humanos aplica en el contexto de la vigilancia estatal de las comunicaciones.

Entre ellos se destacan la Resolución de las Naciones Unidas sobre "El derecho a la privacidad en la era digital,"[22] el Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo,[23] el informe de la Comisión Interamericana de Derechos Humanos sobre el impacto de internet en el derecho a la libertad de expresión,[24] el informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas[25] la Alta Comisionado de las Naciones Unidas para los Derechos Humanos sobre el alcance y la protección del derecho a la privacidad en la era digital,[26] y los dos últimos reportes del nuevo Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas, David Kaye sobre anonimato, cifrado y protección de los denunciantes.[27]

Expertos de la sociedad civil y de la academia han emprendido la labor de estudiar la aplicación del derecho internacional de los derechos humanos vigente en el contexto de la vigilancia de las comunicaciones, fruto de lo cual se han elaborado principios que condensan las normas y la jurisprudencia existente con relación a este tema.

El ejemplo más destacado de esta clase de iniciativas son los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, elaborados por distintos expertos académicos y activistas, que ya han empezado a ser reconocidos por organismos internacionales como doctrina autorizada para interpretar el sentido y alcance de los derechos humanos en el contexto de la vigilancia de las comunicaciones.[28] Tomando en cuenta la jurisprudencia de la Corte Constitucional mencionada antes, en la medida en que estos principios interpretan derechos contenidos en tratados que hacen parte del bloque de constitucionalidad (como la Convención Americana sobre Derechos Humanos o el Pacto Internacional de Derechos Civiles y Políticos), constituyen doctrina relevante para

interpretar esos derechos, sin perjuicio de que algunos de estos principios tengan una fuerza normativa aún mayor por reproducir normas que hacen parte de tratados que integran el bloque de constitucionalidad.

Por último, la Corte Constitucional también ha reconocido relevancia a las decisiones de órganos que aplican tratados de los cuales Colombia no es parte, pero cuyo contenido es similar a otros en los que sí es parte. Es el caso de la Corte Europea de Derechos Humanos, la cual aplica el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales. Según la Corte Constitucional, los pronunciamientos de la Corte Europea de Derechos Humanos son relevantes para analizar la validez de las normas colombianas por lo menos por dos razones: la primera, que la jurisprudencia, tanto nacional como extranjera, es una fuente de interpretación de las normas jurídicas; y la segunda, que si bien Colombia no es parte del Convenio Europeo de Derechos Humanos, varias de las disposiciones de este Convenio se reproducen en tratados que sí resultan vinculantes para Colombia, por lo que sus decisiones son un "*criterio guía útil para efectos de discernir el contenido y alcance de los compromisos internacionales de Colombia en la materia*".

Mencionar la relevancia de las decisiones del citado órgano resulta de interés para el asunto bajo análisis, pues la Corte Europea de Derechos Humanos ha proferido importantes decisiones en materia de vigilancia de las comunicaciones, que pueden arrojar luz sobre las soluciones jurídicas más razonables en los retos que este tema plantea.

## 2.2 Salvaguardas a la vigilancia estatal de las comunicaciones en el derecho internacional

Distintos tratados internacionales que hacen parte del bloque de constitucionalidad consagran salvaguardas a los derechos de las personas frente a la vigilancia de las comunicaciones. Así, el artículo 11.2 de la Convención Americana sobre Derechos Humanos establece que "*[n]adie 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*".

Según la Corte Interamericana de Derechos Humanos, aun cuando el artículo 11.2 de la Convención Americana no lo mencione expresamente, el derecho a la intimidad protege también las conversaciones telefónicas, y "*puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones*".[29]

De acuerdo con este tribunal, para que una injerencia no se considere arbitraria o abusiva debe a) estar prevista en ley, b) perseguir un fin legítimo, y c) ser idónea, necesaria y proporcional.[30] Estas limitaciones han sido definidas de manera general por la Corte Interamericana, pero pueden precisarse acudiendo a lo dispuesto por la Corte Europea de Derechos Humanos. Esta última ha señalado, entre otras, que las medidas de vigilancia deben basarse en una ley que sea particularmente precisa, principalmente por el riesgo implícito de abuso de cualquier sistema de vigilancia secreto y por la continua sofisticación de la tecnología disponible para realizar esas actividades.[31] Así, no serían suficientes autorizaciones de vigilancia generales y vagas contenidas en una ley para entender que se satisface el criterio de legalidad.

También el Pacto Internacional de Derechos Civiles y Políticos protege el derecho a la intimidad, en su artículo 17. Ésta artículo protege a los individuos de injerencias arbitrarias e ilegales en su vida privada. El Comité de Derechos Humanos, órgano encargado de interpretarlo, ha establecido que para que una injerencia no sea considerada arbitraria o ilegal, debe a) estar prevista en la ley, b) estar en consonancia con las disposiciones, propósitos y objetivos del Pacto, y c) ser razonables a la luz de las circunstancias del caso concreto.[32]

Al igual que la Corte Interamericana, el Comité de Derechos Humanos ha sostenido que este derecho no sólo protege la inviolabilidad de las comunicaciones, sino también proscribe la posibilidad de realizar vigilancia y otras clases de intervenciones en la vida privada y familiar de las personas. En este sentido, el Comité de Derechos Humanos ha afirmado que el derecho a la intimidad implica que "*[d]ebe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones*".[33]

Las salvaguardas que impone el derecho internacional para considerar válida una limitación al derecho a la intimidad de las personas están explicadas con detalle en los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* (en adelante, los "Principios"). En ellos no sólo se ratifica que la limitación de las libertades fundamentales debe estar prescrita por la ley y ser proporcional, sino que se explica con detalle el alcance de estas salvaguardas. Estos Principios serán desglosados a lo largo de este reporte.

## 2.3 Salvaguardas constitucionales a la vigilancia estatal de las comunicaciones

El artículo 15 de la Constitución Política colombiana establece el marco jurídico general del derecho a la intimidad, señalando su alcance y la manera como este derecho puede limitarse. Este artículo reconoce tres derechos diferentes: la intimidad, el buen nombre y el habeas

data. La Corte Constitucional ha sostenido en repetidas ocasiones que estos tres derechos son autónomos, ya que protegen ámbitos distintos de la vida de las personas y exigen, por lo tanto, garantías distintas.

En términos generales, la jurisprudencia colombiana ha demarcado el ámbito de protección de estos tres derechos de la siguiente forma.[34] El derecho al buen nombre "*alude al concepto que del individuo tienen los demás miembros de la sociedad en relación con sus comportamiento, honestidad, decoro, calidades, condiciones humanas y profesionales, antecedentes y ejecutorias.*"[35] Por su parte, para ilustrar el contenido del derecho a la intimidad se hace constante alusión a la metáfora de una "*órbita reservada*", la cual se encuentra "*exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad*", cuya protección se considera necesaria para permitir el pleno desarrollo de la vida personal, individual y cultural.[36] Por último, el *hábeas data* se refiere al derecho a conocer, actualizar y rectificar las informaciones que se recojan en bancos de datos y en archivos de entidades públicas y privadas.

Para la Corte Constitucional, la demarcación del contenido de los derechos al buen nombre, a la intimidad y al *hábeas data* es relevante para entender en qué circunstancias estos derechos son desconocidos y cómo puede pedirse su protección a las autoridades. Por ejemplo, con relación al manejo de la información que sobre una persona se tenga, estos derechos pueden vulnerarse por razones distintas. En términos generales, se desconoce el derecho al buen nombre cuando los datos sobre una persona son falsos o erróneos; se desconoce el derecho a la intimidad cuando los datos hacen referencia a aspectos que pertenecen a la órbita reservada que tiene una persona; y se desconoce el derecho al *hábeas data* cuando la información personal contenida en bases de datos ha sido recogida de manera ilegal, es errónea (por falsa o desactualizada) y se relaciona con aspectos propios del ámbito privado de las personas.[37]

El derecho a la intimidad, como cualquier otro derecho fundamental, puede ser limitado.[38] El propio artículo 15 de la Constitución Política señala como regla general que "[l]a correspondencia y demás formas de comunicación privada son inviolables", pero especificando a continuación que estas pueden ser interceptadas o registradas (i) mediante orden judicial y (ii) en los casos y con las formalidades que establezca la ley. En otras palabras, la Constitución exige que haya reserva legal y judicial para la limitación del derecho a la intimidad. Además, el artículo 28 de la Constitución establece que toda persona es libre, y que por lo tanto el domicilio de ninguna persona puede ser registrado, "*sino en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivo previamente definido en la ley*".

Esta regla general tiene una excepción concreta, también establecida en la Constitución Política. Se trata de la facultad que tiene la Fiscalía General de la Nación de realizar

"*registros, allanamientos, incautaciones e interceptaciones de comunicaciones"* sin orden judicial previa, aunque en todo caso especificando que deberá existir un control de legalidad posterior de la actuación. Como se dijo, esta es la única excepción en la que se admite una restricción del derecho a la intimidad sin orden judicial previa. A continuación se explicará con más detalle la regulación de rango legal en la materia.

# III.
# Normativa de rango legal que aborda la vigilancia estatal de las comunicaciones

Antes de proceder al análisis de la legislación colombiana sobre la vigilancia estatal de las comunicaciones, presentaremos un resumen de los sistemas de vigilancia existentes en el país. El informe titulado "Un estado en la sombra" publicado por la ONG defensora del derecho a la privacidad, Privacy International, en agosto de 2015, revela los detalles de las principales plataformas de vigilancia de las comunicaciones en Colombia:[39]

- Esperanza: Éste sistema se utiliza contra una persona específica que se encuentra bajo sospecha, y los equipos son administrados por la Fiscalía. De acuerdo al informe, "Esperanza adolecía de varias vulnerabilidades de seguridad, y su restricción del acceso a datos sólo para objetivos concretos predefinidos y en virtud de una orden judicial."[40]
- Plataforma Única de Monitoreo y Análisis (PUMA): Se presenta como un sistema de monitoreo telefónico e Internet vinculado directamente a la infraestructura de la red, administrado y costeado por la Policía y gestionado por la Dirección de Investigación Criminal e Interpol (DIJIN), la unidad a cargo de la administración judicial. Según el informe, los proveedores de servicios en Colombia no sólo "conocen"de la existencia de PUMA sino que han "colaborado en su instalación", aunque se encuentran " excluidos de su funcionamiento diario."[41]
- Sistema Integral de Grabación Digital (SIGD) de la Dirección de Inteligencia Policial (DIPOL): La DIPOL adquirió sus propias tecnologías de vigilancia estatal de las comunicaciones. Según el informe, el sistema fue construido con el objetivo de deslindar sus actividades de vigilancia como Esperanza de la Fiscalía. El *software* de la DIPOL permite el procesamiento de gran cantidad de datos masivos y generalizado, desde información pública disponible en redes sociales a datos sensibles como los datos biométricos. Estos datos pueden analizar perfiles y determinar patrones de comportamiento a través del tiempo. Según el informe, el sistema "puede recopilar 100 millones de registros de datos de llamada al día e interceptar 20 millones de SMS diarios", datos que luego pueden combinarse con datos biométricos, imágenes, vídeo, entre otros. La DIPOL no están autorizada a realizar actividades de "interceptación" sin la supervisión de la Fiscalía.[42]
- Herramientas de *hackeo*: El informe revela que la DIPOL adquirió programas maliciosos (malware en inglés) que permite infiltrar y controlar un teléfono, dispositivo o computadora de manera remota. La DIJIN tampoco está autorizada a realizar actividades de "interceptación" sin la supervisión de la Fiscalía.

Estos esquemas anteriormente presentados han sido utilizados para conducir vigilancia desde la Dirección de Inteligencia Policial (Dipol) a reconocidos periodistas colombianos que han estado informando al público sobre una supuesta red de prostitución masculina que operaba en el seno de la Policía Nacional denominada como "la comunidad del anillo",[43] que involucra a alféreces, políticos y altos jefes policiales. Este grave caso, que al cierre de esta edición (Marzo 2016) sigue bajo investigación por una comisión presidencial, la Procuraduría General de la Nación y la Fiscalía General de la Nación, provocó las renuncias del Director de la Policía Nacional, Rodolfo Palomino y del viceministro del Interior, Carlos Ferro.[44]

A mediados de diciembre del año 2015 la periodista Vicky Dávila denunció que fue objeto de seguimiento, que sus conversaciones fueron escuchadas y que ocurría lo mismo con su equipo de colaboradores.[45] En referencia a estos casos , la Procuraduría solicitó a la Fundación Karisma una copia de la investigación que realizó junto a Privacy International "Un Estado en la sombra", que revela el uso de malware en el país.[46]

A continuación, analizaremos las distintas circunstancias que permiten a las autoridades registrar o acceder a las comunicaciones privadas de las personas conforme a la normativa colombiana, atendiendo a lo establecido en los artículos 15 de la Constitución Política, 11 de Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos. A continuación se explican estos escenarios.

## 3.1 Vigilancia estatal de las comunicaciones en la legislación penal

La legislación penal regula la vigilancia estatal de las comunicaciones de dos formas. Por una parte, las normas penales procesales establecen los procedimientos que deben seguirse para poder vigilar la comunicación de personas, con el único fin de recolectar pruebas en el marco de un proceso penal. Por otra parte, la legislación penal sustancial tipifica como delito una serie de conductas tendientes a sancionar la vigilancia ilegal de las comunicaciones de las personas.

De acuerdo con el artículo 250 de la Constitución Política, la Fiscalía General de la Nación tiene el deber de asegurar los elementos materiales probatorios en el marco de investigaciones penales, señalando que "*[e]n caso de requerirse medidas adicionales que impliquen afectación de derechos fundamentales, deberá obtenerse la respectiva autorización por parte del juez que ejerza las funciones de control de garantías para poder proceder a ello*". Igualmente, señala que la Fiscalía tiene la facultad de "*[a]delantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones*" sin autorización judicial previa, pero con control judicial posterior dentro de las 36 horas siguientes al registro.

Al interpretar ambas disposiciones, la Corte Constitucional ha dicho que la regla general en el sistema jurídico colombiano es que las decisiones que restringen los derechos fundamentales de los investigados e imputados deben estar previstas en la ley (reserva legal) y ser autorizadas por un juez (reserva judicial),[47] y de manera excepcional, se confiere a la Fiscalía General de la Nación facultades que limitan los derechos de las personas, con la intención de permitir el recaudo de información relevante para los fines de un proceso penal, pero sujeta a un control de legalidad posterior a la actuación. Esta excepción opera sólo para los casos de registros, allanamiento, incautaciones e interceptaciones de comunicaciones, y se justifican por referirse a realidades fácticas que están propensas a cambios repentinos o que pueden ser alteradas fácilmente, lo cual perjudicaría la investigación criminal.[48]

La mencionada excepción debe ser interpretada de manera restrictiva, para evitar que se eluda la garantía de la autorización judicial previa para la afectación de derechos. En virtud de esta regla, por ejemplo, la Corte Constitucional ha sostenido que actuaciones como la búsqueda selectiva de información confidencial de una persona indiciada o sindicada en bases de datos no puede ser considerada una especie de registro, por lo cual ha exigido que para proceder con esta diligencia debe existir una autorización judicial anterior, ya que no cabe dentro de las actividades que pueden realizarse con orden de la Fiscalía General de la Nación sujeta a control judicial posterior.[49]

Así, a la Fiscalía se le permite realizar interceptación de comunicaciones, incautación de equipos y medios de almacenamiento de datos, y realizar seguimiento a personas vinculadas a un proceso penal o a cosas o lugares, solamente con un control judicial posterior a la medida. El Código de Procedimiento Penal establece los casos y las formalidades en los que la Fiscalía puede hacer uso de esta facultad. Al respecto, señala que la interceptación de comunicaciones (i) sólo procederá con el fin de buscar elementos materiales probatorios y evidencia física transmitida mediante cualquier red de comunicación que tengan interés para una investigación penal; (ii) debe fundamentarse por escrito; (iii) no puede dirigirse contra las comunicaciones de un acusado con su defensor; (iv) tienen una vigencia máxima de tres meses; y (v) debe ser sometida a control del juez dentro de las 36 horas siguientes a su expedición.[50]

La legislación procesal penal también establece que "las autoridades competentes" serán las encargadas de la operación técnica de la interceptación y de su procesamiento. A pesar de la vaguedad de la ley en lo relativo a las autoridades encargadas de realizar la operación, la Corte Constitucional la avaló. El argumento que utilizó es que la norma sí especifica la autoridad que da la orden y dirige la interceptación (la Fiscalía General de la Nación), dejándole la posibilidad de determinar las autoridades que realizan la tarea de interceptación y su procesamiento.

Además, aunque la norma no especifica estas "autoridades competentes", pueden ser determinadas a través de una interpretación sistemática de las normas que regulan la operación técnica de la interceptación de comunicaciones. Señala la Corte que el artículo 46 de la ley 938 de 2004 establece que la mencionada competencia recae en las autoridades de policía judicial (actualmente, los órganos que cumplen funciones de policía judicial son el Cuerpo Técnico de Investigaciones y la Policía Nacional).[51]

La Fiscalía General de la Nación también tiene la potestad de ordenar la recuperación de información dejada al navegar por internet u otros medios similares de una persona que sea indiciada o imputada dentro de un proceso penal, cuando se cumplan las siguientes formalidades y situaciones: (i) el fiscal debe tener motivos razonablemente fundados para inferir que el indiciado o imputado ha estado transmitiendo información útil para la investigación que se adelante al navegar por internet u otros medios tecnológicos equivalentes; (ii) el fiscal podrá ordenar la aprehensión de computadores y servidores que pueda haber utilizado, al igual que medios de almacenamiento físico; (iii) la aprehensión se limitará exclusivamente al tiempo necesario para la captura de la información que se busca; y (iv) deberá haber un control judicial dentro de las 36 horas siguientes a la expedición de la orden de aprehensión de equipos.[52]

Además, la Fiscalía tiene la facultad de vigilar a una persona que sea indiciada o imputada en un proceso penal. Para poder hacer uso de esta facultad deben cumplirse las siguientes circunstancias y formalidades: (i) debe existir una autorización previa del Director Nacional o Seccional de Fiscalía; (ii) deben existir motivos razonablemente fundados para inferir que el indiciado o imputado podrá conducir a información útil para la investigación que se adelanta; (iii) el seguimiento podrá darse por un lapso determinado; (iv) en todo caso, si durante el año siguiente a la expedición de la orden de vigilancia no se obtiene ningún resultado, la orden de vigilancia se cancelará, pero podrá expedirse de nuevo si surgen nuevos motivos; (v) en la vigilancia se empleará cualquier medio técnico aconsejable; (vi) la vigilancia tendrá como propósito recaudar información relevante a fin de identificar o individualizar los autores o partícipes, las personas que lo frecuentan, los lugares a donde asiste y aspectos similares, cuidando de no afectar la expectativa razonable de la intimidad del indiciado o imputado o de terceros, y (vii) deberá haber control judicial posterior dentro de las 36 horas siguientes a la expedición de la orden de vigilancia.

Por otro lado, además del Código de Procedimiento Penal, existe otra norma que regula la interceptación de comunicaciones, pero sólo con relación a una situación muy específica: cuando se declare un estado de conmoción interior.[53] Se trata de la ley estatutaria que regula los estados de excepción (ley 137 de 1994), la cual faculta al Gobierno nacional a realizar, durante estados de conmoción interior, interceptaciones o registro de comunicaciones " *con el único fin de buscar pruebas judiciales o prevenir la comisión de delitos"*, siempre y cuando

medie una autorización judicial.[54]

Como se dijo anteriormente, la legislación penal colombiana contempla una serie de delitos que sancionan la vigilancia ilegal de las comunicaciones de las personas. Así, se consagra como delito la interceptación de comunicaciones sin orden judicial –exceptuando, claro está, el caso de la Fiscalía General de la Nación, según lo previsto en el artículo 250 de la Constitución. Al respecto, el artículo 269C del Código Penal establece que "*[e]l que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses*".

Adicionalmente, con ocasión de una reforma al Código Penal realizada en el 2009 con el fin de proteger la información y los datos de las personas, fue agregado un nuevo título a este código. Entre los tipos penales que se establecieron en la reforma se encuentran el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales y la suplantación de sitios web para capturar datos personales.[55]

## 3.2 Vigilancia estatal de las comunicaciones en la legislación de inteligencia y contrainteligencia

Aparte de los procesos penales, el legislador contempló la posibilidades de que se restringieran los derechos de las personas por la vigilancia estatal de sus comunicaciones en el marco de las actividades de inteligencia y contrainteligencia.

En diversas oportunidades la Corte Constitucional ha considerado legítimo que se restrinjan ciertos derechos de las personas, como su intimidad y su libre expresión, por cuenta de la realización de actividades de inteligencia y contrainteligencia. Estas tienen como fin la recopilación, análisis y difusión de información que ayude a los responsables de las políticas y a otras entidades a tomar medidas encaminadas a la protección de la seguridad nacional.[56] Por esto, involucra la vigilancia de las comunicaciones de las personas, con el fin de obtener información sobre factores que puedan amenazar la seguridad nacional.

Debido a la importante finalidad que esta actividad persigue, se ha considerado legítimo que mediante ella se impongan ciertas limitaciones a los derechos de las personas, siempre y cuando estas cumplan con distintos criterios. En términos generales, según ha dicho la Corte Constitucional, "*las atribuciones de los organismos de inteligencia y contrainteligencia deben desarrollarse estrictamente en el marco de la Constitución, el derecho internacional*

*de los derechos humanos y el derecho internacional humanitario".*[57] Por esta razón, para determinar los criterios que deben enmarcar las actividades de inteligencia y contrainteligencia, resulta relevante no solo consultar lo dispuesto por la Constitución colombiana, sino también lo previsto por tratados internacionales y por organismos o instrumentos internacionales encargados de interpretar su contenido.

Al respecto, la Corte Constitucional ha sostenido que las actividades de inteligencia deben (i) estar consagradas en la ley de manera clara y precisa, la cual debe especificar el procedimiento para realizarlas, los funcionarios que pueden autorizarlas y la motivación para autorizarlas; (ii) perseguir fines constitucionalmente legítimos, como la protección de la democracia constitucional, de la seguridad nacional y de la defensa nacional; (iii) ser necesarias, es decir, deben limitarse a las estrictamente indispensables para el cumplimiento de la función; e (iv) incorporar elementos de rendición de cuentas, como la presentación de informes periódicos de inteligencia y contrainteligencia y la de llevar un registro de las acciones autorizadas y de las desarrolladas.[58]

El derecho internacional de los derechos humanos consagra salvaguardas similares a las establecidas por la Corte Constitucional para la realización de actividades de inteligencia y contrainteligencia. Por ejemplo, la Corte Interamericana de Derechos Humanos ha señalado que estas actividades deben respetar los criterios que autorizan la limitación de los derechos humanos, lo cual implica, por ejemplo, que para respetar el derecho a la vida privada, estas actividades deben cumplir estos requisitos: a) estar previstas en ley; b) perseguir un fin legítimo, y c) ser idóneas, necesarias y proporcionales.[59] Además, deben existir controles "*especialmente rigurosos"*, pues las condiciones de reserva en la que operan estos mecanismos implican un riesgo de que deriven en la comisión de violaciones de derechos humanos e ilícitos penales.[60]

Por su parte, los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* ratifican que las medidas que implican vigilancia de las comunicaciones deben estar establecidas por ley, perseguir un fin legítimo, ser idóneas, necesarias y proporcionales, establecer controles (institucionales y no institucionales), garantizar el debido proceso, el derecho al recurso efectivo, la transparencia y las garantías necesarias contra el acceso ilegítimo.

La ley de Inteligencia y Contrainteligencia (ley 1621 de 2013) habilita a las agencias de seguridad la realización de ciertas actividades que suponen una restricción a los derechos de las personas. Esta ley establece cuáles son las agencias que pueden realizar labores de inteligencia y contrainteligencia en Colombia. Según el artículo 3 de esta ley, dicha función la llevan a cabo las dependencias de las Fuerzas Militares y la Policía Nacional organizadas para tal fin, la Unidad de Información y Análisis Financiero, y los demás que faculte la ley. Según dicho artículo, éstos son los únicos organismos que pueden desempeñar tareas de

inteligencia y contrainteligencia.

Entre los organismos que realizan labores de inteligencia en Colombia se encuentran los siguientes: la Dirección Nacional de Inteligencia, creada en el 2011 con el fin de reemplazar al Departamento Administrativo de Seguridad (DAS); Jefatura de Inteligencia y Contrainteligencia Militar Conjunta, que depende del Comando General de las Fuerzas Militares; la Dirección de Inteligencia de la Policía (DIPOL), unidad de la Policía Nacional encargada de la función de producir inteligencia estratégica; la Jefatura de Inteligencia Naval; la Jefatura de Inteligencia y Contrainteligencia del Ejército Nacional; la Jefatura de Inteligencia Aérea. Cabe destacar que también pueden ejercer labores de inteligencia en las Fuerzas Militares las *"unidades o dependencias especiales"* creadas por el Comando General, la Policía Nacional, el Ejército, la Armada o la Fuerza Aérea, mediante acto administrativo.[61]

En particular, la ley 1621 habilita a las agencias de seguridad la realización de las siguientes funciones que limitan los derechos de las personas: (i) monitorear el espectro electromagnético y (ii) requerir a los operadores de servicios de telecomunicaciones información que ayude a la identificación y localización de los usuarios de estos servicios. Esta ley no habilita la interceptación de comunicaciones, pues afirma expresamente que esta se rige de manera exclusiva por las reglas previstas por la Constitución Política y por el Código de Procedimiento Penal en la materia. Se trata, como se mencionó antes, de información que hace parte de la vida privada de las personas, por lo que su revelación constituye una limitación al derecho fundamental a la privacidad. A continuación se explica con más detalle en qué consisten estas dos actividades que pueden ser realizadas por las agencias de inteligencia y que pueden afectar la vida privada de las personas.

La legislación colombiana distingue entonces entre interceptación de comunicaciones y monitoreo del espectro electromagnético. Este último corresponde, en términos de la Corte Constitucional, a una "*labor de rastreo de forma aleatoria e indiscriminada"*, que implica "*la captación incidental de comunicaciones en las que se revelan circunstancias que permiten evitar atentados y controlar riesgos para la defensa y seguridad de la Nación. Técnicamente se estaría ante una especie de rastreo de sombras, imágenes y sonidos representados en frecuencias de radiación electromagnética y ondas radioeléctricas".*[62] Es decir, la normativa Colombiana crea una diferencia legal entre monitorear las comunicaciones con fines de seguridad nacional y el interceptar las comunicaciones conforme a las normas de derecho procesal penal. Valga mencionar que esta definición de "monitoreo del espectro" corresponde a una interpretación jurisprudencial realizada por la Corte Constitucional, y que la ley no consagra ninguna definición específica al respecto.

A diferencia del monitoreo del espectro, la interceptación de comunicaciones implica el seguimiento individualizado de las comunicaciones de una persona, y se hace con el fin de recolectar material probatorio en el marco de un proceso penal, por lo que se rige por las

normas constitucionales y penales.[63]

Con todo, puede afirmarse que la aplicación de las normas de inteligencia hace pensar que el monitoreo del espectro se realiza de una manera mucho más amplia de como la define la Corte Constitucional. Según detalla el informe de Privacy International, distintos organismos en Colombia, como la Dirección de Inteligencia Policial (DIPOL), la Dirección de Investigación Criminal e INTERPOL (DIJIN), y el DAS, hasta su disolución, *"han utilizado dispositivos de interceptación de comunicaciones móviles (conocidos genéricamente como IMSI catchers), que permiten la interceptación localizada indiscriminada de todas las llamadas de teléfonos móviles y mensajes de texto en un lugar específico"*. Estas labores distan de la *"interceptación incidental,"*[64] que es como la Corte entiende el monitoreo de comunicaciones.

Otro aspecto clave de la Ley de Inteligencia y Contrainteligencia tiene que ver con la regulación de los mensajes de voz cifrados. Al respecto, el parágrafo 2 del artículo 44 de esta ley señala que los operadores de servicios de telecomunicaciones deberán ofrecer a los organismos de inteligencia llamadas de voz cifradas. Dicho artículo agrega que este servicio será exclusivo del alto gobierno y de los organismos de inteligencia, lo que implica que la utilización de mensajes de voz cifrados no podrá ser proveído a todas aquellas personas que no sean parte del alto gobierno o de las agencias de inteligencia.

## 3.3 Vigilancia de las comunicaciones en la normativa de telecomunicaciones

La legislación colombiana de telecomunicaciones puede intervenir en el sector de las tecnologías de la información y las comunicaciones para que los obliga a los proveedores de redes y servicios de comunicaciones a permitir el uso de su infraestructura para conducir la vigilancia, condicionando a que esta intervención se haga por razones de "*defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública."*[65]

En desarrollo de esta facultad legal, el Gobierno expidió un decreto imponiendo a los proveedores de redes y servicios de comunicaciones el deber de implementar y garantizar la infraestructura tecnológica necesaria que provea puntos de conexión y de acceso al tráfico, para que las autoridades competentes, previa autorización de la Fiscalía General de la Nación, puedan adelantar las labores de interceptación.[66]

Según el decreto 1704, los proveedores de servicios están obligados a entregar a la Fiscalía "*o demás autoridades competentes",*[67] datos del suscriptor, "*tales como"* su identidad, su dirección de facturación y el tipo de conexión. Allí mismo se dispone que "*los proveedores de redes y servicios de telecomunicaciones deberán mantener actualizada la información de sus suscriptores y conservarla por el término de cinco años".*

Además, en la ley de inteligencia se consagró que las agencias de inteligencia tienen la facultad de requerir a las empresas de telecomunicaciones información sobre a) el historial de comunicaciones de los abonados telefónicos vinculados, b) los datos técnicos de identificación de los suscriptores sobre los que recaen una operación de inteligencia, c) la localización de las celdas en que se encuentran las terminales y d) cualquier otra información que contribuya a la localización.[68]

En otras palabras, se trata de información que no se relaciona con el contenido de las comunicaciones, sino con los datos técnicos sobre estas, mejor conocidos como metadatos, y cuyos datos permiten revelar el contenido de las comunicaciones o inclusive información más sensible. Éstos datos revelan información sobre la identidad de una persona (información sobre el suscriptor o información sobre el equipo móvil), sus interacciones (el origen y el destino de sus comunicaciones,) y su ubicación (los lugares y los horarios, la cercanía a otras personas) y relaciones sociales.[69]

Esta disposición de la ley de inteligencia obliga a entregar los datos técnicos sobre la información allí mencionada, poniendo un plazo máximo de cinco años. Lo interesante es que condiciona su aplicación a que sea "técnicamente viable". Es decir, en esta disposición no existe expresamente una obligación de retener datos, pero si las empresas ya retienen los datos, el gobierno puede solicitar su acceso hasta cinco años máximo. Esto da a entender que debe ya existir una retención voluntaria para que la ley funcione.

# IV.
# ¿Respeta la legislación colombiana los estándares internacionales de derechos humanos en materia de actividades de vigilancia? Algunas propuestas de mejora

La legislación colombiana a la que se ha hecho referencia en el capítulo anterior puede entrar en tensión con el respeto de los derechos humanos identificados al inicio del presente reporte, ya que se aprecia en varios casos una falta de conformidad con los distintos estándares internacionales en materia de vigilancia de las comunicaciones por la autoridad. Se trata de estándares que buscan resguardar en la mayor medida posible el respeto por los derechos humanos potencialmente afectados por tales actividades.

A continuación se contrasta la normativa expuesta con los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, y conforme a las debilidades evidenciadas se presentan algunas recomendaciones de mejora con el fin de promover que la regulación se alinee con tales principios. Ello resulta particularmente pertinente, por cuanto el respeto por los derechos humanos en todo ámbito es un deber que el Estado colombiano ha adquirido al ratificar tratados internacionales en la materia.

## 4.1 Adecuación de la normativa nacional a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

### Legalidad

Conforme con los Principios, toda medida de vigilancia de las comunicaciones que implique una limitación a los derechos humanos debe encontrarse prescrita por ley. Además las normas referidas a vigilancia estatal de las comunicaciones deben cumplir con estándares de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Por último, el principio de legalidad hace conveniente la existencia de mecanismos de revisión periódica por medio de un proceso legislativo o reglamentario de carácter participativo para la actualización de las normas relativas a la vigilancia estatal de las comunicaciones.

Conforme con la normativa Colombiana, el principio de legalidad ha sido consagrado en forma general por la Corte Constitucional a través de la doctrina de reserva legal, el cual establece que las decisiones que restringen los derechos fundamentales de los investigadas e imputadas deben estar previstas en la ley.

Dicho principio de legalidad es respetado en la normativa penal destinada a regular la actividad de vigilancia estatal de las comunicaciones, sin embargo en materia de regulación de actividades de inteligencia y la normativa de las telecomunicaciones, existen situaciones en las cuales no se da cabal cumplimiento al principio.

El principio de legalidad se ha manifestado también en la decisión de la Corte Constitucional acerca de los límites a las actividades de inteligencia, exigiendo que ellas se consagren en la ley de manera clara y precisa, así como los procedimientos para realizarlas, los funcionarios que pueden autorizarlas, y la motivación para autorizarlas. Sin embargo, la ley de inteligencia es vaga y ambigua al regular múltiples materias, desconociendo que las medidas que limitan los derechos de las personas deben estar previstas de manera clara y precisa en la ley, según lo establece el principio de legalidad.

En especial, los fines que dan lugar a la realización de actividades de inteligencia y contrainteligencia (proteger la seguridad nacional, proteger las instituciones democráticas, asegurar la defensa nacional, entre otros) no están definidos. La legislación colombiana tampoco ofrecen ejemplos que ayuden a hacerse una idea más clara acerca de los temas de los que se ocuparán los servicios de inteligencia y contrainteligencia. Esto puede conducir a que, en definitiva, sean las agencias de inteligencia y no el legislador las que terminen definiendo los eventos que dan lugar a la realización de labores de inteligencia y contrainteligencia.

La ley de inteligencia y contrainteligencia también falla al momento de no regular directamente los niveles de clasificación de la información y optar porque el Gobierno se ocupe mediante decreto de este asunto.[70] La Corte Constitucional avaló esta delegación al Gobierno con el argumento que en todo caso la ley da criterios para que se realice la reglamentación.[71] Al delegar la definición de los niveles de clasificación al Gobierno, se le permite que sea la propia rama ejecutiva la que defina los criterios de clasificación de la información de inteligencia, y la propia agencia de inteligencia y contrainteligencia la que aplique esos criterios en los casos concretos.[72] Esta situación desconoce que la reserva de la información, en la medida en que supone una limitación del derecho de acceso a la información, debería estar definida claramente por la ley, conforme lo señala el principio de legalidad.

Adicionalmente, un vacío importante que contiene esta ley consiste en no definir específicamente cuáles son las actividades que pueden ser realizadas por los organismos de inteligencia. Especialmente, con relación al monitoreo del espectro electromagnético, se

observa que se trata de una facultad que tienen las agencias de inteligencia y que está restringida al monitoreo del conjunto de longitudes de onda de todas las radiaciones electromagnéticas.[73] En el caso colombiano, esta facultad no cuenta con una definición legal, (tan solo existe una definición interpretativa realizada por la Corte Constitucional ceñida al espectro electromagnético).

En nuestra opinión, la falta de precisión en la legislación colombiana explica en parte la controversia que ha surgido en Colombia en años recientes acerca del fundamento legal para poner en marcha programas de interceptaciones masivas y automatizadas de las comunicaciones, que efectuarían agencias de inteligencia a través de mecanismos como la Plataforma Única de Monitoreo y Análisis (PUMA) y el Sistema Integral de Grabación Digital (SIGD). La legalidad del empleo de estas herramientas ha sido cuestionada por la propia Fiscalía General de la Nación.[74] Controversias de este estilo pueden ser evitadas mediante leyes claras y concretas, que señalen con precisión la clase de labores de vigilancia que pueden emprenderse y los órganos específicos autorizados a emprenderlas.

La legislación en materia de inteligencia debe en todo caso tener presente la regla constitucional de acuerdo con la cual la interceptación de las comunicaciones de las personas solo puede hacerse de manera individualizada, en el marco de un proceso penal, y con participación de la Fiscalía General de la Nación y de las autoridades judiciales nacionales.

El deber de las empresas de comunicaciones de entregar a los organismos que cumplen funciones de policía judicial información sobre sus suscriptores no está previsto en una ley disponible al público. La norma mediante la cual se obliga a los proveedores de redes y servicios de comunicaciones a entregar información sobre sus suscriptores es un decreto, es decir, no cuenta con la aprobación del órgano democrático ni con la publicidad propia de las leyes. Además de no tener la jerarquía de una ley, no es lo suficientemente precisa, pues no especifica las circunstancias en las que sería procedente esta medida.

No resulta claro tampoco el alcance en material penal de lo que la normativa de telecomunicaciones ordena retener a los proveedores de redes y servicios de comunicaciones: si se limita únicamente a la información sobre la identificación de los usuarios (tales como número de identificación o dirección de correspondencia), o si también cobija la información relacionada con el uso que estos hacen de los servicios contratados (fecha, hora y duración de una comunicación, historial de navegación, personas con quienes se lleva a cabo la comunicación, etc.).

Esta vaguedad se debe a que el decreto 1704 de 2012 no menciona de manera taxativa la información de los usuarios que debe ser conservada por las empresas prestadoras de servicios de internet y de telecomunicaciones, sino que se refiere de manera general a información que permita la identificación de los usuarios, y se limita a mencionar algunos

ejemplos de esta clase de información.

## Objetivo legítimo

Conforme al respeto de los derechos humanos, los Principios ilustran que las medidas de vigilancia estatal de las comunicaciones sólo pueden encontrarse justificadas en forma específica para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante y que sea necesario en una sociedad democrática.

En el caso de Colombia, las normas penales procesales satisfacen el principio al establecer procedimientos que deben seguirse para poder vigilar la comunicación de personas, con el único fin de recolectar pruebas en el marco de un proceso penal.

Del mismo modo, el principio de objetivo legítimo se ha manifestado en la decisión de la Corte Constitucional acerca de los límites a las actividades de inteligencia, exigiendo que ellas persigan fines constitucionalmente legítimos, como la protección de la democracia constitucional, de la seguridad nacional y de la defensa nacional.

En materia de telecomunicaciones las obligaciones de retención de información por los prestadores de servicios no se encuentran justificadas por la facultad del Estado de requerir tales por razones de "defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública".

## Necesidad

Conforme con los Principios resulta necesario que la normativa aplicable a la vigilancia estatal de las comunicaciones limite el alcance de tal actividad a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo identificado por la normativa.

En materia penal, puede constatarse el cumplimiento de este principio en Colombia, por cuanto a la Fiscalía se le permite realizar interceptación de comunicaciones, incautación de equipos y medios de almacenamiento de datos, y realizar seguimiento a personas vinculadas a un proceso penal o a cosas de estas, solo con el fin de buscar elementos materiales probatorios y evidencia física transmitida mediante cualquier red de comunicación que tengan interés para una investigación penal, lo cual debe fundamentarse por escrito, y no puede dirigirse contra las comunicaciones de un acusado con su defensor. Además debe tener una vigencia limitada (máxima de tres meses) y sometida a un control judicial (previo o posterior).

Con relación al principio de necesidad, la legislación en materia de inteligencia y contrainteligencia señala que "La actividad de inteligencia y contrainteligencia debe ser necesaria para alcanzar los fines constitucionales deseados; es decir que podrá recurrirse a esta siempre que no existan otras actividades menos lesivas que permitan alcanzar tales

fines."[75] Igualmente, la decisión de la Corte Constitucional acerca de los límites a las actividades de inteligencia exige que ellas se limiten a las estrictamente indispensables para el cumplimiento de la función legítima identificada.

Por su parte, las normas de vigilancia en materia de telecomunicaciones señalan que las empresas prestadoras de servicios de internet y de telecomunicaciones deberán contar con la infraestructura tecnológica necesaria que provea puntos de conexión y acceso a la captura del tráfico de las comunicaciones que cursen por sus redes. No existe ninguna mención adicional que especifique qué clase de uso se daría a la tecnología, ni una regla que señale que la tecnología que se implemente sea la menos invasiva a la privacidad de las personas.

## Idoneidad

Este Principio se dirige a identificar si los medios dispuestos por la normativa de vigilancia de las comunicaciones en cada país son los adecuados para el objetivo legítimo perseguido.

El principio de idoneidad se encuentra reconocido en la legislación sobre inteligencia y contrainteligencia. Al respecto, el artículo 5 de la ley 1621 de 2013 señala lo siguiente: "La actividad de inteligencia y contrainteligencia debe hacer uso de medios que se adecuen al logro de los fines definidos en el artículo 4o de esta ley; es decir que se deben usar los medios aptos para el cumplimiento de tales fines y no otros". En desarrollo de esta disposición, la ley establece que la información recolectada en ejercicio de actividades de monitoreo del espectro electromagnético que no sirvan para los fines de las actividades de inteligencia debe ser destruida y no podrán ser almacenada en bases de datos.[76] Además, dispone la ley de inteligencia que cada organismo encargado de cumplir estas funciones deberá crear un comité para la corrección, actualización y retiro de datos e información de inteligencia.

Estos comités deberán tomar en cuenta que la información recaudada para fines distintos a los propios de las actividades de inteligencia "será retirada de las bases de datos y archivos de inteligencia, y almacenada en un archivo histórico hasta tanto la Comisión para la depuración rinda su informe de recomendaciones."[77]

## Proporcionalidad

El cumplimiento de los Principios requiere que la normativa de vigilancia de las comunicaciones contenga mecanismos que permitan la ponderación entre la afectación de derechos humanos y las medidas de vigilancia de las comunicaciones autorizadas. Así como la evaluación acerca si los mecanismos contemplados en la normativa son efectivos para verificar que la afectación resulta limitada y razonable al objetivo legítimo identificado, preservando en la mayor medida posible el respeto por los derechos humanos implicados.

El principio de proporcionalidad puede verse recogido en la normativa penal colombiana, por cuanto la Fiscalía General de la Nación al ordenar a través de la aprehensión de equipos

la recuperación de información dejada al navegar por internet u otros medios similares de una persona que sea indiciada o imputada dentro de un proceso penal debe cumplir con acreditar que cuenta con motivos razonablemente fundados para inferir que el indiciado o imputado ha estado transmitiendo información útil para la investigación, debiendo limitarse dicha aprehensión al tiempo necesario para la captura de la información que se busca, y deberá ejercerse un control judicial dentro de las 36 horas siguientes a la expedición de la orden de aprehensión de equipos.[78]

También se encuentra expresamente previsto en la legislación sobre inteligencia y contrainteligencia. La ley 1621 de 2013 lo define así en su artículo 5: "La actividad de inteligencia y contrainteligencia deberá ser proporcional a los fines buscados y sus beneficios deben exceder las restricciones impuestas sobre otros principios y valores constitucionales. En particular, los medios y métodos empleados no deben ser desproporcionados frente a los fines que se busca lograr".

Por el contrario, en la normativa de telecomunicaciones la retención obligatoria de datos está regulada de manera vaga y puede ser altamente desproporcionada. No es claro si el deber que tienen las empresas de comunicaciones y las que prestan servicios de internet de retener datos se refiere exclusivamente a los datos de identificación de las personas, o si abarca también datos relacionados con el uso que estas hacen de los servicios contratados (fecha, hora y duración de una comunicación, historial de navegación, etc.). La retención obligatoria de datos del suscriptor y metadatos es una restricción claramente desproporcionada del derecho a la intimidad, tal como lo argumentó la Corte Europea de Justicia al analizar la directiva europea sobre retención de metadatos.[79]

De acuerdo con la Corte Europea de Justicia, la retención masiva de datos asociada exclusivamente a un periodo limitado de tiempo es una afectación desproporcionada al derecho a la intimidad, pues (i) cobija a la población entera de una nación, cualquier individuo, cualquier medio de comunicación y todos los datos de tráfico sin limitación, diferenciación o excepción; (ii) no contiene un criterio objetivo que permita determinar las circunstancia de acceso a los datos ni un procedimiento para que haya lugar a esto; y (iii) no realiza distinción sobre la duración de la retención de los datos atendiendo a las personas o a la utilidad de los datos retenidos.[80]

Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones apuntan en la misma dirección, al señalar que es una limitación desproporcionada del derecho a la intimidad retener información que no sea relevante para enfrentar una amenaza específica.

## Autoridad competente

El cumplimiento de los Principios en esta materia para brindar el mayor nivel de protección

de los derechos humanos afectados se encuentra asegurado por la intervención en la autorización de una medida de vigilancia de las comunicaciones de una autoridad judicial, imparcial e independiente, que además se encuentre capacitada en materia de tecnología y cuente con los recursos adecuados en el ejercicio de las funciones en esta materia.

La Corte Constitucional ha consagrado en Colombia la regla de reserva judicial, la cual implica que la regla general en el sistema jurídico colombiano es que las decisiones que restringen los derechos fundamentales de los investigados e imputados deben ser autorizadas por un juez.

De conformidad con el artículo 250 de la Constitución Política, la Fiscalía General de la Nación tiene el deber de asegurar los elementos materiales probatorios en el marco de investigaciones penales, señalando que "*[e]n caso de requerirse medidas adicionales que impliquen afectación de derechos fundamentales, deberá obtenerse la respectiva autorización por parte del juez que ejerza las funciones de control de garantías para poder proceder a ello*". Igualmente, señala que la Fiscalía tiene la facultad de "*[a]delantar registros, allanamientos, incautaciones e interceptaiones de comunicaciones*" sin autorización judicial previa, pero con control judicial posterior dentro de las 36 horas siguientes al registro.

Esta excepción opera sólo para los casos de registros, allanamiento, incautaciones e interceptaciones de comunicaciones, y se justifican por referirse a realidades fácticas que están propensas a cambios repentinos o que pueden ser alteradas fácilmente, lo cual perjudicaría la investigación criminal.[81]

El control judicial de actividades de inteligencia resulta limitado a las interceptaciones de comunicaciones, y no aplica para el caso del monitoreo de comunicaciones.

Por último, la normativa de telecomunicaciones no específica como un requisito para la entrega de los datos de identificación de suscriptores la existencia de una orden judicial, con lo cual se ignora la salvaguarda a los derechos de las personas, constituida por la revisión judicial de legalidad y proporcionalidad de la medida.

## Debido proceso

Para la protección de los derechos humanos implicados los Principios requieren la autorización de una medida de vigilancia de las comunicaciones se verifique en el marco de un debido proceso, el cual contemple una audiencia pública u otra forma de comunicación para el afectado, dentro de un plazo razonable (previo o posterior a la autorización de la medida) en un tribunal independiente, competente e imparcial. Asimismo, la existencia de instancias de reconsideración.

Como se ha visto, las medidas de restricción del derecho a la intimidad que se dan en el

marco de un proceso penal están protegidas por la intervención de un juez, bien sea antes de que la medida pueda realizarse o después de que se haya realizado.

En materia de interceptación de comunicaciones o de registro de correspondencia, la persona contra quien se realizaron tales medidas podrá conocer de sus resultados y tendrá la posibilidad de participar en la audiencia de control de legalidad (cuando en el proceso ya haya habido formulación de la imputación) o de solicitar una audiencia con el fin de pedir la exclusión del material probatorio de los resultados de los seguimientos.[82]

## Notificación del usuario

Una salvaguarda exigida por los Principios es que toda medida de vigilancia de las comunicaciones contemple la comunicación al afectado con la oportunidad y la información suficientes para que pueda impugnar la decisión.

En materia penal, este principio se garantiza en la medida en que la persona que fue objeto de actividades de seguimiento tiene la oportunidad de controvertir en audiencias la legalidad de las medidas que se tomaron en su contra. Dependiendo de la etapa en la que se encuentre el proceso penal, el acusado podrá intervenir en la audiencia de legalidad de la medida se seguimiento o solicitar una nueva audiencia para pedir la exclusión de los resultados de estas medidas del material probatorio del proceso.

La normativa de inteligencia no contempla la notificación a los usuarios de la realización de actividades de vigilancia de las comunicaciones en su contra. La notificación es un deber de los Estados que sólo podría suspenderse (más no obviarse) cuando se presenten ciertas circunstancias, según lo dispuesto por los 13 Principios.

En otras palabras, en Colombia una persona no puede consultar si existen o han existido en el pasado acciones de inteligencia en su contra, ni pedir su corrección, ni hay un juez que controle la realización de ciertas actividades de inteligencia que interfieren con sus derechos humanos.

## Transparencia

Los 13 Principios requieren de la implementación de medidas de transparencia en la normativa relativa a la 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. El objetivo es proporcionar a las personas en general la información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la vigilancia de las comunicaciones.

El Principio de Transparencia ha sido reconocido en la decisión de la Corte Constitucional acerca de los límites a las actividades de inteligencia, exigiendo que ellas incorporen elementos de rendición de cuentas, como la presentación de informes periodos de inteligencia y contrainteligencia y la de llevar un registro de las acciones autorizadas y de las desarrolladas.

Sin embargo, la ley de inteligencia no consagra un mecanismo de supervisión pública de las actividades de vigilancia. En cambio, prevé controles internos y externos a las actividades de inteligencia. Entre los externos se cuenta la intervención judicial (limitada a las interceptaciones de comunicaciones, no aplica para el caso del monitoreo de comunicaciones) y un control político, a cargo de la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia. Esta comisión tiene tres funciones principales: hacer control y seguimiento político, verificar el uso eficiente de los recursos y comprobar la legalidad de las actuaciones de los servicios de inteligencia. Las facultades que se le reconocen a la Comisión legal se orientan hacia la revisión del funcionamiento de los mecanismos de control de las actividades de inteligencia.

El parágrafo primero del artículo 22 señala que la Comisión legal podrá reunirse con la Junta de Inteligencia Conjunta, conocer los informes anuales de los inspectores, requerir información adicional a los inspectores y a las oficinas de control interno, citar a los jefes y directores de los organismos de inteligencia y conocer los objetivos nacionales de inteligencia trazados en el Plan Nacional de Inteligencia. Así, para poder verificar la legalidad de las actuaciones de los organismos de inteligencia y contrainteligencia, la Comisión legal tendrá que limitarse a juzgar a partir de la información que esos mismos organismos le provean, lo cual es especialmente grave tratándose de actividades secretas, pues quienes las realizan pueden escudarse en la confidencialidad de la información para no revelar sus conductas.

En materia penal, la transparencia de las medidas de vigilancia por parte de la autoridad se promueve en la medida en que el procedimiento penal está regido por el principio de publicidad. En desarrollo de este principio, las audiencias en las que se controla la legalidad de las interceptaciones de comunicaciones y otras medidas de vigilancia están abiertas al escrutinio público. En todo caso, el principio de publicidad de las actuaciones judiciales admite excepciones consagradas por la ley para proteger derechos fundamentales y desarrollar principios y valores constitucionales.

Específicamente, el artículo 18 de la ley 906 de 2004 señala que el juez puede limitar la publicidad de los procedimientos cuando considere que con ella se "pone en peligro a las víctimas, jurados, testigos, peritos y demás intervinientes; se afecte la seguridad nacional; se exponga a un daño psicológico a los menores de edad que deban intervenir; se menoscabe el derecho del acusado a un juicio justo; o se comprometa seriamente el éxito de la investigación."

## Integridad de las comunicaciones y sistemas

La satisfacción de este Principio requiere que las autoridades nacionales se abstengan de exigir a los proveedores de servicios de comunicación o proveedores de "hardware" o "software" que desarrollen la capacidad de vigilancia o de control en sus sistemas, recoger o retener determinada información exclusivamente para fines de vigilancia por el Estado. La retención o la recopilación de datos *a priori* nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anónimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios.

En esta materia la legislación colombiana de telecomunicaciones prevé que el Estado puede intervenir en el sector de las tecnologías de la información y las comunicaciones para que los proveedores de redes y servicios de comunicaciones provean los servicios y permitan el uso de su infraestructura, condicionando a que esta intervención se haga por razones de "*defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública.*"[83] En desarrollo de esta facultad legal, el Gobierno expidió un decreto imponiendo a los proveedores de redes y servicios de comunicaciones el deber de implementar y garantizar la infraestructura tecnológica necesaria que provea puntos de conexión y de acceso al tráfico, para que las autoridades competentes, previa autorización de la Fiscalía General de la Nación, puedan adelantar las labores de interceptación.

Como fue explicado, la ley 1621 relativa a actividades de inteligencia habilita a las agencias de seguridad requerir a los operadores de servicios de telecomunicaciones información que ayuden a la identificación y localización de los usuarios de estos servicios, pero establece como límite el respeto de las reglas previstas por la Constitución Política y por el Código de Procedimiento Penal en la materia.

También la mencionada ley establece que solo podrán utilizar "mensajes de voz cifrados" quienes sean parte del alto gobierno o de agencias de inteligencia, excluyendo de esta manera que los particulares puedan hacer uso de esta opción. Estas disposiciones afectan seriamente el Principio de Integridad de las Comunicaciones y Sistemas.

## Garantías para la cooperación internacional

Los Principios toman en cuenta la existencia de acuerdos internacionales de asistencia judicial recíproca (MLAT, por sus siglas en inglés) que tengan implicancia en la vigilancia de las comunicaciones, para verificar si se respeta en ellos el principio de mayor nivel de protección disponible para las personas de los países respectivos. Asimismo, sostiene que en el momento en que los Estados procuren asistencia para efectos de hacer cumplir su legislación interna, los Estados deben aplicar el principio de la doble incriminación.

Colombia cuenta con un acuerdo con Francia para el intercambio de información sobre crimen transnacional.[84] Dicho acuerdo contempla en su artículo segundo reglas para el

tratamiento de los datos nominativos (que permiten la identificación de una persona en particular) comunicados por un país a otro como consecuencia de la cooperación acordada. La comunicación de los datos debe hacerse especificando los fines con que ellos deben utilizarse y el periodo de uso. Al final de dicho periodo, los datos deben ser destruidos. Se considera también el intercambio de información a formas de crimen transnacional tales como: terrorismo, lavado de activos, tráfico de estupefacientes, tráfico de armas, falsificación de moneda, trata de personas, tráfico de bienes culturales e ilícitos contra la propiedad intelectual e industrial, y tráfico de recursos naturales.

Colombia cuenta con un tratado sobre intercambio de material de inteligencia con la Organización del Tratado del Atlántico Norte.[85] Este acuerdo establece medidas para el intercambio y protección de la información que sea compartida entre las partes. Algunas de estas medidas incluyen el compromiso de proteger y salvaguardar la información y el material que sea intercambiada entre las partes, lo cual implica asegurar el cumplimiento de procedimientos de seguridad comunes, así como el compromiso de no divulgar información a terceros sin el consentimiento de la parte que origina.

Existe un acuerdo entre Colombia y la Oficina de Policía Europea para el intercambio de todo tipo de información sobre crimen internacional.[86] Entre otras formas de cooperación este Acuerdo cubre el intercambio de información sobre investigaciones de severas formas de crimen internacional, tales como, tráfico de drogas, crímenes relacionados a materiales nucleares, inmigración ilegal, tráfico de personas, crímenes relacionados a vehículos motorizados, falsificación de moneda y lavado de dinero. El Acuerdo contempla una serie de previsiones relativas al propósito del intercambio de información, la forma de transmisión y conservación, así como la posibilidad de clasificar su nivel de confidencialidad, medidas que persiguen limitar y proteger el uso de la información intercambiada.

El convenio internacional para la represión de los atentados terroristas cometidos con bombas[87] contempla algunos acuerdos multilaterales sobre intercambio de información. El convenio prevé que los Estados intercambien información relativa al paradero de presuntos responsables de un delito enunciado en el y tome inmediatamente las medidas que sean necesarias de conformidad con su legislación nacional para investigar los hechos relativos a actos terroristas con explosivos. El convenio también contempla que toda persona que se encuentre detenida o respecto de la cual se adopte cualquier medida o sea encausada con arreglo al convenio goce de un trato equitativo, incluido el goce de todos los derechos y garantías de conformidad con la legislación del Estado en cuyo territorio se encuentre y con las disposiciones pertinentes del derecho internacional, incluido el derecho internacional en materia de derechos humanos.

Existe un acuerdo bilateral entre el Gobierno de la República de Colombia y el Gobierno de la República Federativa del Brasil sobre Cooperación en materia de la defensa.[88] El objetivo

del acuerdo es promover la cooperación entre las Repúblicas de Colombia y Brasil en materia de defensa, en especial en materia de investigación, apoyo logístico, industria aeronáutica, naval y terrestre, intercambio de conocimientos y experiencias y acciones conjuntas de entrenamiento, con el fin de fortalecer la capacidad de respuesta de las autoridades nacionales de ambos países e incrementar el intercambio de experiencias, experticia y fortalezas en las diferentes áreas. Las partes del acuerdo se comprometen a guardar reserva sobre la información y material que sea intercambiado en su contexto.

## Garantías contra el acceso ilegítimo y derecho a recurso efectivo

El estándar de protección de los derechos humanos identificado por los Principios en esta materia requiere que la normativa nacional proteja de forma general la privacidad de las comunicaciones y sancionen la vigilancia de las comunicaciones por parte de actores públicos o privados. Asimismo, requiere que la normativa contenga medios efectivos de reclamo y reparación a las personas afectadas.

La legislación penal colombiana contempla la sanción penal de la vigilancia ilegal de las comunicaciones. Existe un delito la interceptación de comunicaciones sin orden judicial exceptuando, claro está, el caso de la Fiscalía General de la Nación, según lo previsto en el artículo 250 de la Constitución, y en el 2009 se agregaron los tipos penales de acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales y la suplantación de sitios web para capturar datos personales.[89]

Por el contrario, la ley de inteligencia y contrainteligencia no contempla un recurso para la defensa de las personas que crean ser objeto de vigilancia. En efecto, las personas que crean que pueden ser objeto de esta clase de actividades no cuentan con un recurso que les permita verificar si en efecto están siendo objeto de vigilancia, y de ser procedente solicitar su corrección, actualización y en su caso depuración de la información. Ya en el 2009, la Comisión Interamericana de Derechos Humanos le había manifestado su preocupación al Estado colombiano por la ausencia de este recurso,[90] lo cual no fue corregido por la ley 1621 de 2013. La ley 1621 de 2013 se limita a mencionar que existirá una comisión asesora en materia de depuración de archivos de inteligencia, la cual formulará recomendaciones al Gobierno nacional sobre depuración de datos y archivos de inteligencia, que servirán para que el Gobierno "*oriente*" un sistema de depuración de datos y archivos.[91]

La existencia de este recurso es además consistente con la jurisprudencia de la Corte Constitucional, que ha afirmado que "*la reserva opera respecto del contenido de un documento público pero no respecto de su existencia*",[92] lo cual da fundamento a que existe un recurso con el que los ciudadanos puedan indagar sobre la existencia de información en su contra, más allá de que puedan no tener acceso a dicho documento.

La falta de este recurso es aún más sensible si se toma en cuenta que el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recaen una operación de inteligencia, la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a la localización deben ser entregados a las agencias de inteligencia sin que medie control judicial alguno, a pesar de que se trata de información que invade la órbita de privacidad de las personas y debería, por lo tanto, contar con alguna protección judicial.

# V.
# Recomendaciones de mejora

Para ajustar la legislación nacional sobre vigilancia estatal de las comunicaciones a lo dispuesto por el derecho internacional de los derechos humanos existen varias alternativas de acción que pueden ser tomadas en cuenta por la sociedad civil. A continuación se mencionan cuatro recomendaciones, tres de ellas relacionadas con la legislación y los controles a las actividades de inteligencia y contrainteligencia, y una relacionada con los deberes de las empresas de telecomunicaciones de cooperar con las autoridades nacionales.

El ordenamiento jurídico colombiano prevé distintas acciones que permiten controvertir la validez de la legislación colombiana que entra en tensión con el derecho internacional de los derechos humanos. Así, las leyes de la República (como la de inteligencia y contrainteligencia) pueden ser impugnadas mediante la acción de inconstitucionalidad y los decretos (como el que regula la retención de datos) pueden serlo mediante la acción de nulidad simple. También puede, en el marco de un proceso judicial o de una actuación administrativa, plantearse la procedencia de la excepción de inconstitucionalidad, para solicitar la inaplicación de una norma que se considera que desconoce la Constitución.

La acción de inconstitucionalidad resultaría procedente incluso frente a la ley de inteligencia y contrainteligencia (ley 1621 de 2013) que fue revisada en su totalidad por la Corte Constitucional, tomando en cuenta que en su sentencia[93] este tribunal abordó de manera muy escueta distintos aspectos sensibles regulados en esta ley. Ello permitiría un nuevo pronunciamiento del tribunal, en virtud de la cosa juzgada relativa. Así sucede, por ejemplo, con el alcance del deber de colaboración de los operadores de servicios de comunicaciones con organismos de inteligencia, tema en el que no se tocó la posibilidad de que estas empresas realicen retención obligatoria de datos.

Tratándose específicamente de la legislación sobre actividades de inteligencia, la Comisión Asesora para la depuración de archivos de inteligencia puede ser una instancia de incidencia de gran interés, ya que tiene como finalidad elaborar recomendaciones de política en un tema sensible de la vigilancia de las comunicaciones: la depuración de los archivos de inteligencia. En el informe que esta comisión presente al Gobierno nacional puede sugerir importantes ajustes a la legislación de inteligencia, como con relación a la necesidad de que exista un recurso para que las personas puedan solicitar información sobre la existencia de actividades de inteligencia en su contra.

Para fortalecer los controles al funcionamiento de las actividades de inteligencia y contrainteligencia será importante trabajar de la mano de la *Comisión Legal de Seguimiento*

*a las Actividades de Inteligencia y Contrainteligencia.* El fin es aclarar los alcances que debería tener la Comisión para realizar un control adecuado y efectivo a las agencias que prestan estos servicios. Por ejemplo, sería de gran importancia que en su reglamento se aclare quien podrá acceder a información adicional que le entreguen las instituciones de inteligencia y sus mecanismos de control interno, con el fin de hacer que el control que ejerza tenga mayor efectividad.

Como lo argumentó la Comisión Colombiana de Juristas en el proceso de revisión de la ley 1621 de 2013, para ser eficaz:

> "*la Comisión legal debería tener acceso a información que no necesariamente sea entregada por los mismos organismos a los que se pretende controlar, cómo sería el caso de información entregada por miembros de la sociedad civil, o el de aquella información que obtenga la Comisión directamente, mediante la realización de investigaciones iniciadas motu proprio. En este sentido, conviene mencionar que en distintas legislaciones el mecanismo de control parlamentario puede iniciar investigaciones por iniciativa propia, pedir el acceso a cualquier información de inteligencia –y no sólo a aquella entregada por los mecanismos de control internos–, citar a cualquier funcionario de inteligencia y contrainteligencia, y no solo a los jefes o inspectores".*[94]

La legislación colombiana es particularmente ambigua con relación al alcance del deber que tienen las empresas de telecomunicaciones de colaboración mediante el suministro de información, por lo que su alcance debe ser precisado. El artículo 44 de la ley 1621 consagra el deber de las empresas de telecomunicaciones de suministrar a las agencias de inteligencia datos sobre las comunicaciones de sus suscriptores, y en todo caso las agencias limitarán la solicitud a un periodo no mayor de 5 años. Esto implica que para que funcione este mandato las empresas de telecomunicaciones ya deben contar con la tecnología de almacenamiento de datos por ese periodo. No obstante, no se sabe qué sucede con las empresas que aún no cuentan con esa tecnología, ni qué sucedería con la empresa que la tuviera pero quisiera dejar de utilizarla, etc. Estos interrogantes deben ser resueltos por la ley.

Tampoco se tiene claridad sobre el alcance de la norma que dispone que "los proveedores de redes y servicios de telecomunicaciones deberán mantener actualizada la información de sus suscriptores y conservarla por el término de cinco años". Es preciso que se especifique con claridad que ésta disposición no involucra una obligación de conservar datos sobre las comunicaciones o metadatos, pues implicaría una intromisión desproporcionada en varios de los derechos fundamentales de los colombianos y colombianas.

# VI.
# Conclusión

Las recientes revelaciones a nivel internacional de la intensidad y ámbito en el cual las distintas autoridades ejercen actividades de vigilancia de las comunicaciones han comenzado a despertar el interés de la sociedad civil de limitar la acción de la autoridad para garantizar el adecuado respeto por los derechos humanos que pueden verse vulnerados en el ejercicio de tales actividades de vigilancia.

El logro de este objetivo plantea retos de distinta naturaleza: el más básico consiste en comprender la manera como el plano nacional regula las medidas de vigilancia de las comunicaciones por la autoridad para entender qué es legal y qué no lo es, hasta las más complejas, como la de identificar la forma en la cual dicha normativa se aplica en el día a día, dado el vertiginoso avance de las tecnologías que permiten la vigilancia.

El presente reporte tiene la finalidad de servir como herramienta para avanzar en la evaluación y discusión acerca de las salvaguardas necesarias de implementar en Colombia para proteger los derechos de las personas frente a la realización de actividades de vigilancia por la autoridad. Con ese fin, han expuesto las normas que facultan a distintos organismos del Estado a realizar labores de vigilancia de las comunicaciones de las personas, con el ánimo de reportar esquemática y comprensiva el marco legal que las regula.

La evaluación anterior ha considerado también la jurisprudencia judicial nacional e internacional, así como la práctica administrativa en la aplicación de la normativa identificada, con el objeto de identificar las respuestas que hasta hoy han sido provistas a la problemática de compatibilizar la normativa y prácticas de vigilancia estatal de las comunicaciones con el respeto de los derechos humanos.

En segundo lugar, este reporte avanza en las recomendaciones pertinentes a la adecuación de la normativa nacional a los estándares definidos a nivel internacional para la adecuada protección de los derechos humanos en las actividades de vigilancia estatal de las comunicaciones.

Si bien el legislador ha emprendido la valiosa tarea de abordar distintos aspectos sobre vigilancia de las comunicaciones (penalizando el acceso ilegal a datos y comunicaciones, regulando las actividades de inteligencia, entre otros), en ocasiones estas regulaciones son imprecisas, incompletas, o insuficientes, o en otras oportunidades aún no se ha ocupado de esta tarea porque se la ha encomendado al ejecutivo (como en la definición de los niveles de clasificación de la información de inteligencia, por ejemplo). Lo anterior plantea un serio

riesgo para derechos como la intimidad, la libertad de asociación o la libertad de expresión, por lo que deben ser tomados en cuenta por las autoridades competentes con el ánimo de brindar todas las salvaguardas necesarias a los derechos humanos.

La inactividad por parte del Estado colombiano frente a los problemas identificados pondría en entredicho su compromiso con el reconocimiento y respeto de los derechos humanos en el contexto internacional.

1 Frank La Rue, Reporte del Relator Especial de las Naciones Unidas para la protección del derecho a la libertad de expresión y de opinión, Naciones Unidas, A/HRC/23/40, 17 de abril de 2013, párr. 33, disponible en: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

2 En este sentido, la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sostuvo que "las revelaciones acerca de la vigilancia digital masiva han suscitado interrogantes acerca de hasta qué punto tales medidas son consistentes con los estándares jurídicos internacionales y sobre si se requieren salvaguardas más fuertes para proteger los derechos humanos". El derecho a la privacidad en la era digital, A/HRC/27/37, Alta Comisionada de las Naciones Unidas para los De- rechos Humanos, 30 de junio de 2014, párr. 15, disponible en: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G14/068/74/ PDF/G1406874.pdf?OpenElement

3 El Departamento Administrativo del Servicio de Inteligencia Colombiano fue creado mediante el Decreto 2872 del 31 de octubre de 1953, disponible en: https://www.redjurista.com/documents/d2872_53.aspx

4 Ley Estatutaria Nº1621, de 17 de abril de 2013, por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%20 17%20DE %20ABRIL%20DE%202013.pdf

5 Artículo 2.1 de la Convención Americana sobre Derechos Humanos y artículo 2.2 del Pacto Internacional de Derechos Civiles y Políticos.

6 Entre otros, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos se pronunció sobre esta práctica y la describió en los siguientes términos: "En 2009 se hizo público que el DAS, entidad de inteligencia dependiente de la Presi- dencia de la República, había estado desarrollando, por lo menos desde 2003 y de manera generalizada y sistemática, una serie de actividades ilegales dirigidas contra, entre otros, defensores de derechos humanos, opositores políticos, periodistas y altos funcionarios del Gobierno, como el Vicepresidente. Además, información preocupante publicada en los medios de comunicación indicaría que incluso los magistrados de la Corte Suprema fueron objeto de vigilancia. La Comisión Interamericana de Derechos Humanos, un Relator Especial de las Naciones Unidas y la Oficina en Colombia fueron también objeto de vigilancia. Estas acciones, en muchos casos, tenían como objetivo neutralizar las labores desarrolladas por las víctimas, a quienes se consideraba"blancos legítimos"por ser potenciales opositoras de las políticas gubernamentales". Informe anual de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre la situación de los derechos humanos en Colombia, documento A/HRC/13/72, 4 de marzo de 2010, párr. 14, disponible en: http://www.hchr.org.co/documentoseinformes/informes/altocomisionado/Informe2009_esp.pdf

7 ¿Alguien espió a los negociadores de La Habana?, Revista Semana, 3 de febrero de 2014, disponible en: http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

8 El video del 'hacker' y Zuluaga, Revista Semana, 17 de mayo de 2014, disponible en: http://www.semana.com/nacion/articulo/el-video-del-hacker-con-oscar-ivan-zuluaga/388438-3

9 El Tiempo, Unidad Investigativa, Estos son los correos que prueban seguimientos a Vicky Dávila, 7 de diciembre de 2015, disponible en: http://www.eltiempo.com/politica/justicia/pruebas-de-seguimientos-a-vicky-davila/16451812

10 Privacy International, Demanda y Oferta: La industria de vigilancia al descubierto en Colombia, setiembre 2015, disponible en: https://www.privacyinternational.org/node/638. Ver también el segundo informe de Privacy International, Un estado en la sombra: vigilancia y orden público en Colombia, Agosto 2015, disponible en: https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

11 El Tiempo, Fiscalía le dice 'no' a sistema de interceptación 'Puma' de la Policía,30 de agosto de 2015, disponible en: http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

12 *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* (2014). Disponible en: https://es.necessaryandproportionate.org/text [Accedido 6 de Septiembre, 2015]; Ver también La Rue Frank, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, A/HRC/23/40, 17 Abril, 2013, pág 3.

13 Por cuestiones de forma, en el texto se utilizan como sinónimos las expresiones "intimidad" y "privacidad". A nuestro entender, ambas hacen referencia al mismo derecho, y se distinguen en que una es utilizada en el plano internacional (donde se habla del derecho a la "vida privada") y la otra en el plano nacional (donde se habla del derecho a la intimidad).

14 Jaime Rodríguez v. Iván Mejía Alvarez, sentencia T-1319, Corte Constitucional, 7 de diciembre de 2001, disponible en: http://www.corteconstitucional.gov.co/relatoria/2001/t-1319-01.htm

15 Revisión constitucional del "Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949, relativo a la pro- tección de las víctimas de los conflictos armados sin carácter internacional (Protocolo II)" hecho en Ginebra el 8 de junio de 1977, y de la Ley 171 del 16 de diciembre de 1994, por medio de la cual se aprueba dicho Protocolo, sentencia C-225, Corte Constitucional, 18 de mayo de 1995, disponible en: http://www.corteconstitucional.gov.co/relatoria/1995/C-225-95.htm

16 Para un análisis comprehensivo de la doctrina del bloque de constitucionalidad, ver Carlos Ernesto Molina demanda de inconstitucionalidad contra el artículo 19 (parcial) del Código Sustantivo del Trabajo, sentencia C-401, Corte Constitucional, 14 de abril de 2005, disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2005/C-401-05.htm, y Rodrigo Uprimny Yepes, Bloque de constitucionalidad, derechos humanos y nuevo procedimiento penal, Escuela Judicial Lara Bonilla, Consejo Superior de la Judicatura, Bogotá, 2006.

17 En múltiples ocasiones la Corte Constitucional ha utilizado decisiones de la Comisión Interamericana de Derechos Humanos para interpretar las normas relevantes para su decisión.

18 Ver Ernesto Rey Cantor demanda de inconstitucionalidad contra los artículos 2º (parcial), 3º (parcial), 5º, 6º (parcial) 7º literales c) y f), 8º inciso tercero, 10, 11 (parcial), 13 inciso primero, 14, 15 (parcial), 19 y 20 literal f) de la Ley 74 de 1966, "por la cual se reglamenta la transmisión de programas por los servicios de radiodifusión", sentencia C-010, Corte Constitucional, 19 de enero de 2000, disponible en: http://www.corteconstitucional.gov.co/relatoria/2000/c-010-00.htm, en la que la Corte afirmó que "en la medida en que la Carta señala en el artículo 93 que los derechos y deberes constitucionales deben interpretarse 'de conformidad con los tratados internacionales sobre derechos humanos ratificados por Colombia,' es indudable que la jurisprudencia de las instancias internacionales, encargadas de interpretar esos tratados, constituye un criterio hermenéutico relevante para establecer el sentido de las normas constitucionales sobre derechos fundamentales".

19 En varias ocasiones la Corte Constitucional ha otorgado carácter relevante a las decisiones del Comité de Derechos Humanos, y en algunos casos le ha dado carácter vinculante. Por ejemplo, en un caso sobre libertad de expresión, sostuvo la Corte: "para efectos del presente caso, el bloque de constitucionalidad relativo a la libertad de expresión ha de estar integrado por las normas internacionales, en particular el Pacto de San José y la Convención Internacional de Derechos Civiles y Políticos, junto con las interpretaciones que de tales textos han presentado la Comisión Interamericana de Derechos Humanos, la Corte Interamericana de Derechos Humanos y Comité de Derechos Humanos de Naciones Unidas.También ha de otorgarse un peso distinto a las opiniones, pues la naturaleza judicial de la Corte Interamericana de Derechos Humanos, y su competencia sobre Colombia, implica

que sus opiniones, más que tenidas en cuenta, no pueden ser ignoradas internamente". Rodríguez v. Alvarez, sentencia T-1319, Corte Constitucional, 2001. Ver, además, sentencias C-872 de 2003, C-370 de 2006, T-391 de 2007, C-728 de 2009, entre otras.

20 Ver, entre otras, sentencias C-370 de 2006, T-821 de 2007 y C-579 de 2007. En la sentencia T-821 de 2007, con relación a los Principios Rectores de los Desplazamientos Internos, consagrados en el Informe del Representante Especial del Secretario General de Naciones Unidas para el Tema de los Desplazamientos Internos de Personas y los Principios sobre la restitución de las viviendas y el patrimonio de los refugiados y las personas desplazadas, la Corte sostuvo que "hacen parte del Bloque de constitucionalidad en sentido lato, en tanto son desarrollos adoptados por la doctrina internacional, del derecho fundamental a la reparación integral por el daño causado". Rosmira Serrano Quintero v. Agencia Presidencial para la Acción Social y la Cooperación Internacional, sentencia T-821, Corte Constitucional, 5 de octubre de 2007, disponible en: http://www.corteconstitucional.gov.co/relatoria/2007/t-821-07.htm

21 Así, por ejemplo, respecto de los Principios de Limburgo y los de Maastricht, relacionados con las obligaciones de los Esta- dos en materia de derechos económicos, sociales y culturales, elaborados por expertos en la materia, la Corte Constitucional ha sostenido que "no tiene fuerza vinculante directa, aunque pueden ser empleados como una herramienta interpretativa del alcance de los derechos establecidos en el PIDESC y en el Protocolo de San Salvador y de las obligaciones del Estado colombiano en la materia. Estos últimos sí instrumentos internacionales que hacen parte del bloque de constitucionalidad". Carlos Rodríguez Díaz demanda de inconstitucionalidad contra los artículos 25, 26, 28 y 51 (en lo acusado) de la Ley 789 de 2002, "Por la cual se dictan normas para apoyar el empleo y ampliar la protección social y se modifican algunos artículos del Código Sustantivo del Trabajo", sentencia C-257, Corte Constitucional, 12 de marzo de 2008, disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2008/C-257-08.htm. En otra ocasión, refiriéndose a los Principios de Chapultepec, a los de Johannesburgo y a los de Lima en materia de libertad de expresión, sostuvo que "si bien en principio no integran el bloque de constitucionalidad, en todo caso constituyen doctrina relevante para interpretar los tratados internacionales que hacen parte del mismo", Zonia Betancourt Rojas y Gabriela Fuquene Betancourt v. Policía Nacional, Corte Constitucional, sen- tencia T-511, de 18 de junio de 2010, disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2010/T-511-10.htm

22 Resolución de la Asamblea General de las Naciones Unidas, El derecho a la privacidad en la era digital, UN Doc. A /RES/68/167, 18 de Diciembre de 2013, disponible en: https://eff.org/UN-A-RES-68-167

23 Ben Emerson, Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, UN Doc. A /69/397, disponible en: https://eff.org/A-69-397.

24 Catalina Botero, Informe anual de la Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos, OEA/Ser.L/V/II.149, 31 de diciembre de 2013, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_ia_2013_esp_final_web.pdf

25 Frank La Rue, Reporte del Relator Especial de las Naciones Unidas para la protección del derecho a la libertad de expresión y de opinión, (2013).

26 El derecho a la privacidad en la era digital (2014).

27 David Kaye, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión que aborda la utilización del cifrado y el anonimato en las comunicaciones digitales, UN Doc. A/HRC/29/32, disponible en: https://eff.org/A-HRC-29-32.

28 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponibles en: https://es.necessaryandproportionate.org/analisislegal Ver también EFF, ARTICLE19, Análisis Jurídico Internacional de Apoyo y Antecedentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal, Access, Guía de Implementación Universal de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://s3.amazonaws.com/access.3cdn.net/a0ea4423a1607c836a3_aqm6iyi2u.pdf

29 Escher y otros v. Brasil, Excepciones Preliminares, Fondo, Reparaciones y Costas, Corte Interamericana de Derechos Humanos, sentencia de 6 de julio de 2009, Serie C No. 200, párr. 114.

30 Tristán Donoso v. Panama, Excepción Preliminar, Fondo, Reparaciones y Costas, Corte Interamericana de Derechos Humanos, sentencia de 27 de enero de 2009, Serie C No. 193, párr. 55.

31 Uzun v. Alemania, Caso No. 35623/05, Corte Europea de Derechos Humanos, sentencia de 2 de Septiembre de 2010, párr. 61; Weber y Sarabia v. Alemania. Caso No. 54934/00, sentencia de 29 de Junio de 2006. párr. 93.

32 Comité de Derechos Humanos, Observación General No. 16, Artículo 17 - Derecho a la Intimidad, párr. 4.

33 Id., párr. 8.

34 Véase Juan Carlos Upegui Mejía, Habeas data. Fundamentos, naturaleza, régimen, Ed. Universidad Externado de Colom- bia, Bogotá, 2008.

35 German Colonia y Ana Mercedes Marin v. Administración de la Unidad Residencial "Los Nogales", sentencia T-228, Corte Constitucional, 10 de mayo de 1994, disponible en: http://www.corteconstitucional.gov.co/relatoria/1994/T-228-94.htm

36 Rosa Estelia Peña Carabalí v. Caleb Antonio Avendaño Mosquera, sentencia T-787, Corte Constitucional, 18 de agosto de 2004, disponible en: http://www.corteconstitucional.gov.co/relatoria/2004/t-787-04.htm

37 Corte Constitucional, sentencias T-129 de 2010, T-067 de 2007, T-411 de 1995, entre otras.

38 La jurisprudencia sobre el carácter no absoluto de los derechos fundamentales es abundante. En una de las sentencias en las que la Corte [Constitucional] se refirió a este aspecto, manifestó: "los derechos fundamentales, no obstante su consagración constitucional y su importancia, no son absolutos y, por tanto, necesariamente deben armonizarse entre sí con los demás bienes y valores protegidos por la Carta, pues, de lo contrario, ausente esa indispensable relativización, la convivencia social y la vida institucional no serían posibles" Corte Constitucional, sentencia C-239 de 1997.

39 Ver también una infografía explicando a detalle los programas de vigilancia elaborada por la Fundación Karisma, Sistemas de vigilancia en Colombia al descubierto, disponible en: https://karisma.org.co/sistemas-de-vigilancia-en-colombia-al-descubierto/

40 Privacy International, Un estado en la sombra: vigilancia y orden público en Colombia, página 8, Agosto 2015, disponible en: https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

41 Privacy International, Un estado en la sombra: vigilancia y orden público en Colombia, Agosto 2015, disponible en: https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

42 Privacy International, Demanda y Oferta: La industria de vigilancia al descubierto en Colombia, setiembre 2015, disponible en: https://www.privacyinternational.org/node/638.

43 Crisis en la Policía: todos perdieron. Revista Semana. 20 de Febrero de 2016 http://www.semana.com/nacion/articulo/vicky-davila-palomino-y-ferro-escandalo-en-la-policia/461249

44 Las investigaciones pendientes en el escándalo de la Policía. El Tiempo. 18 de Febrero de 2016 http://www.eltiempo.com/politica/justicia/claves-para-entender-el-escandalo-de-la-comunidad-del-anillo-de-la-policia/16513163

45 Las pruebas de las 'chuzadas' a periodistas sí existen. LA F.m. 18 de Diciembre de 2015 http://www.lafm.com.co/justicia/noticias/los-correos-an%C3%B3nimos-enviados-196561

46 Colombia's new spying scandal: Time for real change. Privacy International. 8 de Marzo de 2016. https://www.privacyinternational.org/node/800

47 Pedro Pablo Camargo demanda de inconstitucionalidad contra el numeral segundo y el parágrafo del artículo 2, el numeral tercero del artículo 3 y el inciso primero del artículo 5 del Acto Legislativo No.03 de 2002, "por el cual se reforma la Constitución Nacional", sentencia C-1092, Corte Constitucional, 19 de noviembre de 2003, disponible en: http://www.corteconstitu- cional.gov.co/relatoria/2003/C-1092-03.htm

48 Alejandro Decastro González demanda de inconstitucionalidad contra los artículos 14 (parcial), 244 (parcial) y 246 (parcial) de la Ley 906 de 2004 "Por la cual se expide el Código de Procedimiento Penal", sentencia C-336, Corte Constitucional, 9 de mayo de 2007, disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

49 Id.

50 Artículos 235 y 237 del Código de Procedimiento Penal. Este término de 36 horas resulta de las 12 que tiene la policía judicial para informar al fiscal que emitió la orden de interceptación, sumadas a las 24 horas que tiene el fiscal para realizar el control de legalidad ante un juez penal. Véase Gustavo Gallón y otro demanda de inconstitucionalidad contra los artículos 14, 15 (parcial) y 16 de la Ley 1142 de 2007, "por medio de la cual se reforman parcialmente las Leyes 906 de 2004, 599 de 2000 y 600 de 2000 y se adoptan medidas para la prevención y represión de la actividad delictiva de especial impacto para la convivencia y seguridad ciudadana", sentencia C-131, Corte Constitucional, 24 de febrero de 2009 (en la cual realizó el estudio de constitucionalidad del artículo 237 de la ley 906 de 2004), disponible en: http://www.corteconstitucional.gov.co/ RELATORIA/2009/C-131-09.htm

51 Dagoberto José Lavalle demanda de inconstitucionalidad contra el artículo 52 (parcial) de la Ley 1453 de 2011 "por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad", sentencia C-594, Corte Constitucional, 20 de agosto de 2014, disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2014/C-594-14.htm

52 Artículos 236 y 237 del Código de Procedimiento Penal.

53 De acuerdo con la Constitución (artículo 213), el estado de conmoción interior se declara "[e]n caso de grave perturbación del orden público que atente de manera inminente contra la estabilidad institucional, la seguridad del Estado, o la convivencia ciudadana, y que no pueda ser conjurada mediante el uso de las atribuciones ordinarias de las autoridades de Policía".

54 Esta norma fue avalada por la Corte Constitucional en la Revisión constitucional del proyecto de ley estatutaria No. 91/92 Senado y 166/92 Cámara "Por la cual se regulan los estados de excepción en Colombia", sentencia C-179,

13 de abril de 1994, disponible en: http://www.corteconstitucional.gov.co/relatoria/1994/C-179-94.htm

55 Ley 1273 de 2009.

56 Retomando la definición contenida en la recopilación de buenas prácticas en materia de inteligencia y contrainteligencia de las Naciones Unidas. Revisión de constitucionalidad del proyecto de ley estatutaria número 263/11 Senado y 195/11 Cá- mara, "Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras dispo- siciones", sentencia C-540, Corte Constitucional, 12 de julio de 2012, disponible en: http://www.corteconstitucional.gov.co/ relatoria/2012/c-540-12.htm

57 Id.

58 Id.

59 Donoso v. Panamá, Corte Interamericana de Derechos Humanos (2009), párr. 56; Escher v. Brasil. Corte Interamericana de Derechos Humanos (2009), párr. 116.

60 Myrna Mack Chang v. Guatemala, Serie C No. 101, Corte Interamericana de Derechos Humanos, sentencia de 25 de no- viembre de 2003, párr. 284. En similar sentido, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Caso no. 62540/00, Corte Europea de Derechos Humanos, sentencia de 28 de junio de 2007, párr. 77.

61 Decreto 857 de 2014, *"por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones""*, artículo 1.

62 Sentencia C-540, Corte Constitucional (2012).

63 Id.

64 Privacy International, *Un Estado en la sombra: vigilancia y orden público en Colombia*, agosto de 2015, disponible en: https://www.privacyinternational.org/sites/default/files/ShadowState_Espanol.pdf

65 Ley 1341 de 2009.

66 Decreto 1704 de 2012.

67 La expresión "o demás autoridades competentes" fue suspendida provisionalmente por el Consejo de Estado, mientras se pronuncia de fondo sobre este asunto, argumentando que permitir que otras autoridades distintas a la Fiscalía ejerzan la facultad de requerir información a las empresas de comunicaciones puede vulnerar la ley 1453 de 2011 y la Constitución Política. Consejo de Estado – Sección Primera, número de radicado 11001-03-24-000-2013-00018-00, magistrado ponente Guillermo Vargas Ayala, 31 de Julio de 2013.

68 Artículo 44 de la ley 1621 de 2013.

69 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text, EFF, ARTICLE19, Análisis Jurídico Internacional de Apoyo y Antecendentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal, Access,

Guía de Implementación Universal de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf

70 Artículo 37 de la ley 1621 de 2013.

71 Sentencia C-540, Corte Constitucional (2012).

72 El Gobierno nacional reglamentó los niveles de clasificación de la información de inteligencia y contrainteligencia mediante el decreto 857 de 2014.

73 Comisión Europea, Comité Científico, Definiciones Técnicas – Glosario, disponible en: http://ec.europa.eu/health/opinions/es/lamparas-bajo-consumo/glosario/def/espectro-electromagnetico.htm

74 El Tiempo, "Fiscalía le dice 'no' a sistema de interceptación 'Puma' de la Policía", 30 de agosto de 2014, disponible en: http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

75 Artículo 5 de la ley 1621 de 2013.

76 Artículo 17 de la ley 1621 de 2013.

77 Artículo 31 de la ley 1621 de 2013.

78 Artículos 236 y 237 del Código de Procedimiento Penal.

79 Esta directiva obligaba a los Estados a asegurarse de que se retuvieran los datos de tráfico y localización, así como los necesarios para la identificación de una persona, por un periodo no menos de seis meses ni mayor de dos años. Directiva 2006/24/EC del Parlamento y del Consejo Europeo, 15 de marzo de 2006, disponible en: http://eur-lex.europa.eu/LexUri- Serv/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

80 Judgment in Joined Cases C - 293/12 and C - 594/12 Digital Rights Ireland and Seitlinger and Others, disponible en: http://curia.europa.eu/juris/documents.jsf?num=C-293/12

81 Alejandro Decastro González demanda de inconstitucionalidad contra los artículos 14 (parcial), 244 (parcial) y 246 (parcial) de la Ley 906 de 2004 "Por la cual se expide el Código de Procedimiento Penal", sentencia C-336, Corte Constitucional, 9 de mayo de 2007, disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

82 Artículos 237 y 238 de la ley 906 de 2004.

83 Ley 1341 de 2009.

84 Acuerdo Bilateral entre el Gobierno de la República de Colombia y el Gobierno de la República Francesa relativo a la Cooperación en Materia de Seguridad Interior, firmado el 22 de julio de 2003 y en vigor desde el 1 de junio de 2007, disponible en: http://apw.cancilleria.gov.co/tratados/SitePages/VerTratados.aspx?IDT=a9ce1083-1d7e-474d-b4df-3501f0bf1ed9

85 Acuerdo entre la República de Colombia y la Organización del Tratado del Atlántico Norte sobre Cooperación y Seguridad de Información, firmado el 25 de junio de 2013 y promulgado a través de la ley 1734 de 8 de septiembre de 2014, disponible en: http://apw.cancilleria.gov.co/tratados/SitePages/VerTratados.aspx?IDT=d65b4217-9bd1-44eb-bbcb-b121ee78e829

86 Agreement on Operational and Strategic Co-operation between Colombia and the European Police Office, firmado el 17 de febrero de 2014 y en vigor desde el 25 de febrero de 2014, disponible en: https://www.europol.europa.eu/content/agree- ment-operational-and-strategic-co-operation-between-colombia-and-european-police-office

87 Resolución A/RES/52/164 adoptada por la organización de las Naciones Unidas el 15 de diciembre de 1997, a la cual se adhirió el Estado colombiano mediante la Ley 804 de 2003, disponible en: http://www.oas.org/juridico/mla/sp/per/sp_per_Con_inter_repr_aten_terro_come_bombas.pdf

88 Suscrito en Bogotá, el 19 de julio de 2008 y promulgado mediante la Ley 1517 de 2012.

89 Ley 1273 de 2009.

90 Informe anual de la Comisión Interamericana de Derechos Humanos 2009, 30 diciembre 2009, documento OEA/Ser.L/V/II, Capítulo IV, párr. 137, disponible en: http://www.cidh.oas.org/annualrep/2009sp/cap.4Colo.09.sp.htm

91 El artículo 30 de la ley 1621 de 2013 señala que "El Gobierno Nacional pondrá en marcha, dentro del año siguiente a la rendición del informe de la Comisión, un sistema de depuración de datos y archivos de inteligencia y contrainteligencia, orientado por el informe de recomendaciones de la Comisión".

92 Franky Urrego Ortiz Demanda de inconstitucionalidad contra la Ley 1097 de 2006, sentencia C-491, Corte Constitucional, 27 de junio de 2007, disponible en: http://www.corteconstitucional.gov.co/relatoria/2007/c-491-07.htm

93 Sentencia C-540, Corte Constitucional (2012).

94 Comisión Colombiana de Juristas, Concepto de constitucionalidad en la revisión del proyecto de ley estatutaria 263 de 2011 Senado – 195 de 2011 Cámara, disponible en: http://www.slideshare.net/Coljuristas/concepto-de-constitucionalidad-en-la-re- visin-del-proyecto-de-ley-estatutaria-263-de-2011-senado-195-de-2011-cmara