Principios Internacionales Sobre la Aplicación de los Derechos Humanos a la Vigilancia de Comunicaciones y el Sistema Interamericano de Protección de Derechos Humanos

Juan Carlos Lara
Valentina Hernández
Katitza Rodríguez

Agosto 2016

ELECTRONIC FRONTIER FOUNDATION

DERECHOS DIGITALES
América Latina

Tabla de contenidos

Introducción

La rápida evolución de las tecnologías de comunicación digital ha brindado a personas de todo el mundo una habilidad sin precedentes para compartir pensamientos e ideas, organizar actividades —ya sean políticas o de otra índole— y de comunicarse con seres queridos con mayor frecuencia que nunca. Sin embargo, estos beneficios traen aparejados grandes desafíos. Así como se incrementan las capacidades de vigilancia del gobierno, también aumentan las amenazas y los desafíos en relación con los derechos humanos.

Cada vez que utilizamos un teléfono, una computadora, u otro tipo de aparato tecnológico, dejamos atrás grandes cantidades de información personal que puede revelar nuestras afiliaciones políticas y religiosas, estados de salud, intereses sexuales, y patrones de comportamiento. Aquellos avances tecnológicos que celebramos le brindan a los Estados herramientas nuevas y más eficientes para la recolección y el análisis de rastros de datos abundantes. Hoy en día, los Estados pueden monitorear, recopilar, almacenar y analizar nuestras comunicaciones e interacciones con nuestros familiares, colegas y amigos a través del tiempo, a veces, sin límites legales precisos, ni garantías adecuadas que eviten cualquier abuso de poder. Las recientes revelaciones que confirman la vigilancia de comunicaciones digitales por parte del Estado, incluyendo la vigilancia masiva, hacen notar hasta qué punto los derechos humanos se ven amenazados en estas situaciones.

Por lo tanto, es urgente que los Estados aprueben leyes de vigilancia nacionales actualizadas y que revisen sus prácticas de vigilancia digital para poder garantizar el cumplimiento de los estándares internacionales en derechos humanos y la protección de la privacidad y de libertades fundamentales en general.

Estas preocupaciones sirvieron de inspiración para la elaboración de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de Comunicación (en adelante también “los 13 Principios” o “los Principios”), que establecen un marco para la aplicación del derecho internacional de los derechos humanos en el contexto de la vigilancia de las comunicaciones en la era digital. Los 13 Principios se encuentran, por tanto, firmemente arraigados en el derecho internacional de los derechos humanos y la jurisprudencia comparada. Esto incluye la jurisprudencia de la Corte Interamericana de Derechos Humanos, en sus interpretaciones de la Convención Americana sobre Derechos Humanos. En algunos casos, los Principios buscan llenar el vacío que existe en el derecho internacional.

Los 13 Principios, entonces, representan quizás el paso más importante dado desde la sociedad civil encaminado a exigirles a los Estados el cumplimiento de estándares

internacionales de derechos humanos en la realización de actividades de vigilancia en la era digital.

En ese sentido, el propósito final del presente trabajo es poner en consideración de la Comisión Interamericana de Derechos Humanos, una guía útil que sistematiza el derecho internacional aplicable, y una explicación de los estándares relevantes y las bases jurídicas para tales estándares.

A continuación se explica cuáles son estos estándares y cuál es su fundamento legal.

I.

El Principio de Legalidad

> *Cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Dado el ritmo de los cambios tecnológicos, las leyes que limitan el derecho a la privacidad deben ser objeto de revisión periódica por medio de un proceso legislativo o reglamentario de carácter participativo.*

El principio de legalidad exige que cualquier restricción a un derecho fundamental sea autorizada por la ley. Dado el importante rol que tienen los derechos de libertad de expresión, de reunión, y de asociación en una sociedad democrática, las leyes de vigilancia deben autorizar a los gobiernos a acceder a comunicaciones e información personal únicamente bajo las circunstancias excepcionales que defina la legislación. Cuando se invoque la seguridad nacional como razón para vigilar, la ley debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resulta legítimo.

Este principio se encuentra reconocido de manera general en el artículo 30 de la Convención Americana sobre Derechos Humanos, que establece:

> *Artículo 30. Alcance de las Restricciones. Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas.*

Al interpretar el artículo 30 de la Convención Americana, la Corte ha hecho una interpretación del sentido del término "leyes". Al respecto, ha sostenido que:

> *[L] palabra leyes en el artículo 30 de la Convención significa norma jurídica de carácter general, ceñida al bien común, emanada de los órganos legislativos constitucionalmente previstos y democráticamente elegidos, y elaborada según el procedimiento establecido por las constituciones de los Estados Partes para la formación de las leyes.*[1]

Con base en el artículo 30 de la Convención Americana, la Corte ha sostenido que la

autorización mediante ley es un requisito indispensable que debe tener toda restricción a un derecho. Ha sostenido que toda restricción a un derecho debe cumplir las siguientes condiciones:[2]

- Que se trate de una restricción expresamente autorizada por la Convención y que cumpla con las condiciones particulares en que ha sido permitida;
- Que los fines de la restricción sean legítimos, es decir, que obedezcan a "razones de interés general" y no se aparten del "propósito para el cual han sido establecidas" (...); y
- Que tales restricciones estén dispuestas por las leyes y se apliquen de conformidad con ellas.

Esto significa que las condiciones y circunstancias generales conforme a las cuales se autoriza una restricción al ejercicio de un derecho humano determinado deben estar claramente establecidas por ley. La norma que establece la restricción debe ser *una ley en el sentido formal y material* y debe existir en consonancia con las restricciones que la propia Convención permite.

La importancia cardinal y el rigor que el sistema interamericano otorga al principio de legalidad en el contexto de vigilancia estatal queda de manifiesto en el caso *Escher y otros vs. Brasil,* el cual analiza el artículo 11 de la Convención Americana sobre Derechos Humanos, y hace referencia a la responsabilidad internacional de Brasil por haber violado el derecho a la privacidad mediante la interceptación, el monitoreo, y la divulgación de llamadas telefónicas de miembros de una organización de interés público (una organización social), tareas llevadas a cabo por la Policía Militar del estado de Paraná.[3] En ese caso, la Corte puso énfasis en los varios componentes de la legalidad, incluyendo las normas legales de pertinencia, competencia, y procedimiento. La Corte mantuvo que, debido a que estos requisitos no se cumplieron, ni siquiera debieron considerarse otros principios cruciales, como el del propósito y la necesidad de la interceptación. La Convención Americana y la interpretación que le da la Corte exigen una ley en el sentido material y formal. En sentido afín, la declaración conjunta del Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y de la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA señala que:

> *[L]los Estados deben garantizar que la intervención, recolección y uso de información personal, incluidas todas las limitaciones al derecho de la persona afectada a acceder a información sobre las mismas, estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados. La ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas,*

las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación.

Dos cuestiones adicionales surgen respecto del principio de legalidad. La primera se relaciona con el acceso de las personas a la normativa que regula el derecho a la privacidad, y la segunda tiene que ver con la actualización de ésta.

De acuerdo con los Principios, no solo debe existir legislación que se ocupe del derecho a la privacidad, sino que esta también debe ser accesible, para garantizar que las personas la conozcan y las revisen y comenten a través de audiencias públicas y el proceso legislativo, que refleja con precisión la protección de los intereses en relación con el respeto y la garantía de los derechos humanos.

Además, como ya lo sostuvo el Relator Especial para la promoción y protección de la libertad de opinión y expresión de Naciones Unidas, las propuestas legislativas para la revisión o la adopción de restricciones a la seguridad individual en línea "deben ser objeto de debate público y ser adoptadas según el procedimiento legislativo ordinario, público, informado y transparente. Los Estados deben promover en dicho debate y procesos, la participación efectiva de una amplia variedad de actores de la sociedad civil y grupos minoritarios y evitar la adopción de esa legislación en virtud de procedimientos legislativos acelerados".[4]

Es necesaria también la revisión y actualización de la legislación que permite injerencias en el derecho a la privacidad para que sea aplicable a esta era digital y de avances tecnológicos. Esto conlleva especial importancia debido a la posibilidad de obsolescencia de los sistemas normativos y a que el Estado puede tener pocos o ningún límite para invadir las libertades fundamentales de los individuos.

Finalmente, cabe señalar la importancia del principio de legalidad respecto de las facultades de vigilancia de las cuales se dota a los órganos de persecución e investigación criminal. Así, dado que el sujeto investigado normalmente desconoce que aquellas medidas están siendo utilizadas para rastrear su actividad, es de suma relevancia contar con una debida redacción, publicidad y comprensibilidad de la norma que habilita su uso. En efecto, la Declaración Conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, de los Relatores de libertad de expresión y opinión de Naciones Unidas y la *Comisión Interamericana de Derechos Humanos* sugirió que los Estados difundan, por lo menos, "información relativa al marco regulatorio de los programas de vigilancia; los órganos encargados para implementar y supervisar dichos programas; los procedimientos de autorización, de selección de objetivos y de manejo de datos...."[5]

II.

Objetivo Legítimo

> *Las leyes sólo deberían permitir la Vigilancia de las Comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.*

En los 13 Principios, la referencia al objetivo legítimo es formulada en dos sentidos: primero, como finalidad en términos positivos, que se basan en proponer que las leyes permitan la vigilancia de las comunicaciones para alcanzar cierto objetivo legítimo; y segundo, como finalidad en términos negativos, que rechazan a la discriminación como factor para ejercer vigilancia.

En el primer sentido, se exige que la vigilancia de las comunicaciones se realice solamente "para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática". En términos afines, el *Artículo 30* de la Convención Americana establece que las restricciones a los derechos en ella consagrados "no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas". Asimismo, el *Artículo 32.2* de dicho instrumento establece que:

> *"los derechos de cada persona están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bien común, en una sociedad democrática".*

La Corte ha indicado, a propósito del alcance de este artículo, que:

> *29. El requisito según la cual las leyes han de ser dictadas por razones de interés general significa que deben haber sido adoptadas en función del "bien común" (art. 32.2 [de la Convención Americana]), concepto que ha de interpretarse como elemento integrante del orden público del Estado democrático, cuyo fin principal es "la protección de los derechos esenciales del hombre y la creación de circunstancias que le permitan progresar espiritual y materialmente y alcanzar la felicidad"(Declaración Americana de los Derechos y Deberes del Hombre).*[6]

La Corte Interamericana de Derechos Humanos (Corte IDH) se explayó sobre estos artículos para enfatizar que una apelación generalizada sobre el bien común no es un objetivo legítimo específico suficiente:

> *[D]e ninguna manera podrían invocarse el "orden público" o el "bien común" como medios para suprimir un derecho garantizado por la Convención o para desnaturalizarlo o privarlo de contenido real (ver el art. 29.a) de la Convención). Esos conceptos, en cuanto se invoquen como fundamento de limitaciones a los derechos humanos, deben ser objeto de una interpretación estrictamente ceñida a las "justas exigencias" de "una sociedad democrática" que tenga en cuenta el equilibrio entre los distintos intereses en juego y la necesidad de preservar el objeto y fin de la Convención.*[7]

En consonancia con esta jurisprudencia, los 13 Principios buscan una delimitación que permita excluir conceptos demasiado vagos —como el de "seguridad nacional"— de las razones que justificarían la restricción al derecho a la privacidad.

Los objetivos legítimos para la restricción a los derechos fundamentales suelen estar vinculados de forma específica con cada uno de ellos. Ocurre así, por ejemplo, respecto de la libertad de manifestar la religión y creencia (Artículo 12.3 de la Convención), de la libertad de pensamiento y expresión (Artículo 13.2 de la Convención), de la libertad de asociación (Artículo 16.2 de la Convención), de la propiedad privada (Artículo 21.1 de la Convención), del ejercicio del derecho de circulación y residencia (Artículo 22.3 de la Convención) y de los derechos políticos (Artículo 23.2 de la Convención).

En cambio, los objetivos legítimos invocados para justificar la vigilancia se refieren a finalidades como la seguridad nacional, el orden público y la salud pública, entre otros. En la Convención Americana no existen menciones de este tipo para las restricciones al derecho a la privacidad, pero en todo caso se entiende que aplican las reglas generales previstas en los artículos 30 y 32 de dicho instrumento, mencionados anteriormente.

Adicionalmente, los 13 Principios establecen que la vigilancia de comunicaciones "no debe aplicarse de manera que discrimine con base en la raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición". Esto implica que la protección de la privacidad no discrimina en razón de las condiciones personales de los posibles afectados. Se trata de una consecuencia lógica de la protección en condiciones de igualdad y de no discriminación de los derechos humanos reconocidos por los tratados internacionales, previsto en los Artículos 1.1 (respecto a la protección o garantía de un derecho convencional) y 24 (respecto a una protección igual de la ley interna o su aplicación) de la Convención Americana. Además, la Convención Interamericana contra toda forma de discriminación e intolerancia reconoce esta

prohibición de discriminación. Incluye también principios de no discriminación, es decir, de no distinción, exclusión, restricción, o preferencia en el ámbito de la vida pública o privada.[8] Finalmente, en los casos en los que se suspenden las garantías debido a amenazas a la independencia o seguridad de los Estados, el artículo 27 de la Convención Americana deja en claro que dichas restricciones no están relacionadas con la discriminación en razón de raza, color, sexo, idioma, religión, u origen social. En otras palabras, incluso en casos en los que se declare estado de emergencia, los Estados no pueden restringir los derechos de manera discriminatoria.

III.

Idoneidad

> *Cualquier caso de Vigilancia de las Comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.*

El acto de vigilancia de las comunicaciones que lleve adelante el Estado debe ser "apropiado para cumplir el objetivo legítimo específico identificado". La interpretación de la Corte del *Artículo 11.2* de la Convención Americana, en los términos ya referidos, da cuenta de lo mismo: las restricciones deben ser idóneas, esto es,[9] ser adecuadas para cumplir su función de protección de otros derechos.[10]

En el sistema interamericano, la Corte Interamericana de Derechos Humanos se ha referido de forma específica a la idoneidad a propósito del derecho a la libertad de expresión, y por tal ha entendido la "capacidad de contribuir a la realización" del objetivo de salvaguardar un bien jurídico.[11] Entonces, en virtud del principio de idoneidad, una medida restrictiva del derecho a la vida privada debe tener la capacidad de contribuir al objetivo legítimo que se persigue, como podría ser, por ejemplo, contribuir a una investigación penal o a la seguridad nacional.

IV.

Necesidad

> *Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La Vigilancia de las Comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.*

De acuerdo con el principio de necesidad, aún en presencia de un objetivo legítimo en los términos del segundo principio, debe expresarse y probarse por parte del Estado que existe una relación de necesidad entre ese objetivo y la vigilancia de comunicaciones.

El artículo 11.2 de la Convención Americana sobre Derechos Humanos reafirma el Principio de Necesidad:

> *"El derecho a la vida privada no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias; por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática."*[12]

Al interpretar el artículo 11.2, la Corte IDH reconoció de manera explícita el Principio de Necesidad en el fallo *Chaparro Álvarez y Lapo Íñiguez vs Ecuador* (2007) en los siguientes términos:

> *"(...) no es suficiente que toda causa de privación o restricción al derecho a la libertad esté consagrada en la ley, sino que es necesario que esa ley y su aplicación respeten los requisitos que a continuación se detallan, a efectos de que dicha medida no sea arbitraria: i) que la finalidad de las medidas que priven o restrinjan la libertad sea compatible con la Convención. Valga señalar que este Tribunal ha reconocido como fines legítimos el asegurar que el acusado no impedirá el desarrollo del procedimiento ni eludirá la acción de la justicia; ii) que las medidas adoptadas sean las idóneas para cumplir con el fin perseguido; iii) que sean necesarias, en el sentido de que sean absolutamente indispensables para conseguir el fin deseado y que no*

> *exista una medida menos gravosa respecto al derecho intervenido entre todas aquellas que cuentan con la misma idoneidad para alcanzar el objetivo propuesto. Por esta razón el Tribunal ha señalado que el derecho a la libertad personal supone que toda limitación a éste deba ser excepcional, y iv) que sean medidas que resulten estrictamente proporcionales, de tal forma que el sacrificio inherente a la restricción del derecho a la libertad no resulte exagerado o desmedido frente a las ventajas que se obtienen mediante tal restricción y el cumplimiento de la finalidad perseguida."*[3]

De acuerdo con la Corte, la "necesidad" de una medida implica que no exista otra menos gravosa para la privacidad de las personas que también sea adecuada para lograr la finalidad propuesta.

V.

Proporcionalidad

La Vigilancia de las Comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la Vigilancia de las Comunicaciones deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia.

Esto requiere que un Estado, como mínimo, deba demostrar lo siguiente a una autoridad judicial competente antes de la realización de la Vigilancia de las Comunicaciones para hacer cumplir la ley, la protección de la seguridad nacional, o la recolección de inteligencia:

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

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

3. Que otras técnicas de investigación menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada resultaría la menos invasiva en la práctica. Y;

4. Que la información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza especifica al fin legitimo alegado; y

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

6. Que la información será accedida solo por la autoridad especificada y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización; y

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

La proporcionalidad exige una ponderación entre la entidad del bien jurídico que sirve de objetivo legítimo, y la entidad de la restricción del derecho afectado. De acuerdo con este principio, debe existir proporción entre la procedencia y extensión de la vigilancia de comunicaciones y el interés de las libertades fundamentales del afectado, incluso en casos que van más allá de la recolección de información (por ejemplo, en el intercambio de información entre organismos estatales). Los 13 Principios enumeran una serie de criterios que sirven para realizar la ponderación entre la vigilancia de las comunicaciones y la protección de los derechos de las personas, como son: la probabilidad de ocurrencia de un delito grave, la probabilidad de obtener evidencia mediante la vigilancia, la inexistencia o inutilidad de medidas menos invasivas, la limitación del objeto de vigilancia, la eliminación de información excedente, el acceso y uso por autoridad específica competente de tal información, y la protección de derechos fundamentales en su esencia.

La Corte Interamericana de Derechos Humanos ha declarado que la restricción a un derecho consagrado en la Convención sólo puede aceptarse si tal restricción es proporcional: de hecho, este análisis recibe el nombre de "test de proporcionalidad". En el caso *Kimel vs. Argentina* (2008), la Corte IDH especificó en qué consiste este análisis:

> *"83. En este último paso del análisis se considera si la restricción resulta estrictamente proporcional, de tal forma que el sacrificio inherente a aquella no resulte exagerado o desmedido frente a las ventajas que se obtienen mediante tal limitación."*[14]

El Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo explica con claridad el principio de proporcionalidad frente a los derechos a la privacidad y a la honra (previstos en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos), señalando que dicho principio implica que la restricción debe tratarse del "instrumento menos perturbador de los que permitan conseguir el resultado deseado y debe guardar proporción con el interés que se desea proteger."[15]

La proporcionalidad como criterio para el control de las potestades estatales es ampliamente citada en la jurisprudencia. Profundizando en su contenido, y citando jurisprudencia de Europa, la Corte Interamericana ha abundado sobre la proporcionalidad en relación estrecha con los requisitos de necesidad e idoneidad. Al respecto, ha señalado en opinión consultiva:

> *Entre varias opciones para alcanzar ese objetivo [legítimo] debe escogerse aquélla que restrinja en menor escala el derecho protegido. Dado este estándar, no es suficiente que se demuestre, por ejemplo, que la ley cumple un propósito útil u oportuno; para que sean compatibles con la Convención las restricciones deben justificarse según objetivos colectivos*

que, por su importancia, preponderen claramente sobre la necesidad social del pleno goce del derecho que el artículo 13 garantiza y no limiten más de lo estrictamente necesario el derecho proclamado en el artículo 13. Es decir, la restricción debe ser proporcionada al interés que la justifica y ajustarse estrechamente al logro de ese legítimo objetivo.[16]

VI.

Autoridad Judicial Competente

Las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. La autoridad debe:

1. Estar separada e independiente de las autoridades encargadas de la Vigilancia de las Comunicaciones.

2. Estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos, y

3. Tener los recursos adecuados en el ejercicio de las funciones que se le asignen.

Los 13 Principios exigen que debe ser una autoridad judicial competente, capacitada, imparcial e independiente la que tome las decisiones sobre la procedencia de acciones de vigilancia de comunicaciones.

Las autoridades que apoyan al sistema interamericano exigen lo mismo. El artículo 8.1 de la Convención Interamericana establece lo siguiente:

> *Toda persona tiene derecho a ser oída (...) por un juez o tribunal competente, independiente e imparcial, establecido con anterioridad por la ley, en la sustanciación de cualquier acusación penal formulada contra ella, o para la determinación de sus derechos y obligaciones de orden civil, laboral, fiscal o de cualquier otro carácter.*

La Corte Interamericana de Derechos Humanos ha interpretado en sentido amplio este derecho. Se entiende así que el Artículo 8 "no establece el derecho a un recurso", correspondiente al artículo 25 de la Convención, sino un derecho al acceso a la justicia, y a la forma en que ella se imparte, con autoridades judiciales independientes e imparciales, tanto para el juzgamiento como para determinar derechos y obligaciones de cualquier carácter.

Como ha dicho la Corte:

> *"El Estado tiene la responsabilidad de consagrar normativamente y de asegurar la debida aplicación de las garantías del debido proceso legal ante*

> *las autoridades competentes, que amparen a todas las personas bajo su jurisdicción contra actos que violen sus derechos fundamentales o que conlleven a la determinación de los derechos y obligaciones de estas."*[17]

La Corte Interamericana ha abundado en el requisito de independencia, señalando que es obligación del Estado protegerlo en dos sentidos: "tanto en su faceta institucional, esto es, en relación con el Poder Judicial como sistema, así como también en conexión con su vertiente individual, es decir, con relación a la persona del juez específico."[18]

Respecto de la imparcialidad, la Corte Interamericana, tomando como referencia la jurisprudencia de la Corte Europea de Derechos Humanos, ha expresado que esta exige que:

> *"el juez que interviene en una contienda particular se aproxime a los hechos de la causa careciendo, de manera subjetiva, de todo prejuicio y, asimismo, ofreciendo garantías suficientes de índole objetiva que permitan desterrar toda duda que el justiciable o la comunidad puedan albergar respecto de la ausencia de imparcialidad",*

Igualmente, ha agregando que:

> *"el juez debe aparecer como actuando sin estar sujeto a influencia, aliciente, presión, amenaza o intromisión, directa o indirecta, sino única y exclusivamente conforme a -y movido por- el Derecho."*[19]

Dos aspectos de los 13 Principios refuerzan estas garantías. El primero exige una autoridad judicial incluso en ausencia de litigación activa —por ejemplo, el requerimiento de que el juez apruebe todas las solicitudes de vigilancia, incluidas las órdenes de allanamiento. La Corte IDH ha apoyado también esta interpretación. E n *Escher vs. Brasil*, la Corte, al referirse a la medida de interceptación de comunicaciones telefónicas por parte de la Policía Militar, manifestó que "la motivación y fundamentación deben demostrar que han sido ponderados todos los requisitos legales y demás elementos que justifican la concesión o la negativa de la medida."[20]

Blanco y Salmón (2012)[21] observan que en este párrafo recién citado se encuentra una precisión muy necesaria que la Corte Interamericana no había realizado antes. En casos anteriores la Corte había afirmado que:

> "*la fundamentación de un fallo debe mostrar a las partes que han sido oídas y que han sido tomados en cuenta sus alegatos. Si bien esto no es posible en un procedimiento sin audiencia de parte, ello no exime a la autoridad del deber de motivar. Por el contrario, le exige realizar una evaluación estricta del cumplimiento o no de los supuestos legales para conceder la medida.*"[22]

La intervención judicial a la hora de autorizar medidas intrusivas de derechos fundamentales

es clave, y no solo en aquellos casos en que se esté ante un juicio oral penal, sino que en todo tipo de procedimiento jurisdiccional, tal y como indica el artículo 8.1 de la Convención Americana de Derechos Humanos, y en cualquier etapa del mismo, ya sea una gestión prejudicial, como en la tramitación del mismo o ejecución de lo decidido. Incluso en la etapa investigativa previa a la participación de un órgano jurisdiccional. Asimismo, es claro que los jueces deben intervenir y motivar toda decisión que signifique tal detrimento en los derechos del individuo.

Es necesaria la existencia de una Autoridad Judicial Competente especialmente en los casos de vigilancia masiva, dados los efectos negativos que tiene sobre los derechos fundamentales.

Los 13 Principios exigen también un nivel de conocimiento para la toma de decisiones en cuestiones de vigilancia de comunicaciones, con jueces "familiarizados con las tecnologías pertinentes y con los principios de derechos humanos a fin de que comprendan adecuadamente la naturaleza de cada solicitud de vigilancia y sean capaces de evaluar su posible impacto en la intimidad individual".[23]

VII.

Debido Proceso

> *El debido proceso exige que los Estados respeten y garanticen los derechos humanos de las personas asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general. Específicamente, al decidir sobre sus derechos, toda persona tiene derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley, salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos, debe buscarse una autorización con efecto retroactivo dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo.*

La legitimidad de la vigilancia de comunicaciones también depende del cumplimiento de reglas concretas de debido proceso, incluyendo garantías sobre el procedimiento y el tribunal competente. Refleja así lo dispuesto en el Artículo 8 de la Convención Americana sobre Derechos Humanos. El Principio sobre Debido Proceso concurre con el principio anterior, relacionado con la participación de una autoridad judicial independiente e imparcial. Se entiende entonces que no basta con que una autoridad judicial autorice una medida de vigilancia de comunicaciones para que esta sea legítima, sino que además se debe actuar en el marco de un proceso que reconozca ciertas garantías mínimas a las personas.

Este principio plantea la posibilidad de que por razones de "riesgo inminente para la vida humana" sea posible prescindir del derecho de las personas a una audiencia pública y justa, pues en este caso la urgencia de la situación no permitiría llevarla a cabo. En todos los demás casos, este principio le impide al Estado pasar por alto el derecho a audiencia pública y justa.

Por eso, el Principio de Debido Proceso es una hipótesis distinta de la suspensión general de garantías propia de los estados de excepción, prevista en el Artículo 27 de la Convención Americana. También es distinta en cuanto a la posibilidad de llevar a cabo procedimientos a puertas cerradas que el Artículo 8.1. de la Convención Americana contempla con respecto a determinados procesos penales. De esta forma, los 13 Principios acuden a sustentar la acción de emergencia, pero la limita a un objetivo legítimo muy específico, como es el "riesgo inminente para la vida humana", excluyendo así consideraciones de conceptos vagos o

ambiguos como la “seguridad nacional”.

Asimismo, los 13 Principios establecen su propia salvaguarda en acciones de emergencia, como por ejemplo: la autorización judicial retroactiva dentro de un plazo razonable y factible. Los 13 Principios dejan claro que el riesgo de fuga o de destrucción de pruebas no debe considerarse suficiente para justificar la autorización con efecto retroactivo en casos de emergencia.

Este requisito refleja lo provisto por el artículo 8 de la Convención Americana sobre Derechos Humanos, el cual establece el derecho de todas las personas a audiencia pública, con las debidas garantías y dentro de un periodo de tiempo razonable, llevada a cabo por una corte competente, independiente e imparcial, previamente establecida por ley.

VIII.
Notificación del usuario

Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados de la decisión de autorizar la Vigilancia de Comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación solo se justifica en las siguientes circunstancias:

1. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; y

2. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y

3. El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.

La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones deben tener la libertad de notificar a las personas de la Vigilancia de las Comunicaciones, ya sea de forma voluntaria o bajo petición.

El Principio de Notificación del Usuario desempeña un papel fundamental en la lucha contra la vigilancia estatal abusiva y el litigió estratégico.

Actualmente, el Estado posee herramientas que permiten el acceso remoto a los archivos y equipos de los individuos a los cuales se desea investigar, no pudiendo éstos percibir que están siendo vigilados por parte de las autoridades. Tal vigilancia es problemática, no sólo por la grave vulneración al derecho a la privacidad y por las nocivas repercusiones que causa en el derecho a la libertad de expresión, sino también porque repercute de forma directa en el derecho al debido proceso, ya que el afectado se ve imposibilitado a recurrir ante una autoridad judicial a alegar la legalidad de la medida.

En el caso *Castillo Petruzzi vs. Perú* (1999), la Corte Interamericana de Derechos Humanos llamó la atención sobre el tipo de medidas que se pueden utilizar para lograr los objetivos de seguridad y combate al crimen, estableciendo que no siempre el fin justifica los medios:

> *"Tal como lo ha señalado este Tribunal, está más allá de toda duda que el Estado tiene el derecho y el deber de garantizar su propia seguridad. Tampoco puede discutirse que toda la sociedad padece por las infracciones a su orden jurídico. Pero por graves que puedan ser ciertas acciones y por culpables que puedan resultar los reos de determinados delitos, no cabe admitir que el poder pueda ejercerse sin límite alguno o que el Estado pueda valerse de cualquier procedimiento para alcanzar sus objetivos, sin sujeción al derecho o a la moral. Existe un amplio reconocimiento de la primacía de los derechos humanos, que el Estado no puede desconocer sin violentar."*[24]

En la era digital, las personas guardan sus documentos y comunicaciones en formato digital —por lo general se guardan en la nube o de otra manera, bajo la custodia de otros. Las proveedoras de telefonía y acceso a Internet ocupan una posición clave en la vigilancia de las comunicaciones, pues transmiten y almacenan las comunicaciones de la mayoría de la población. A menudo conocen la identidad de la persona que crea un sitio web o que deja mensajes en plataformas de redes sociales. Si el Estado desea conocer la identidad de un usuario de Internet, se la solicita a la empresa intermediaria. En ese sentido, si la persona afectada desea impugnar la solicitud de acceso a datos por parte del Estado, ella puede hacerlo únicamente si es notificada por el intermediario o por el gobierno.

Así, este Principio busca proveer información suficiente a la persona afectada sobre la decisión que autoriza la vigilancia para que pueda impugnar la medida o buscar otros remedios efectivos. Así pues, el principio de la notificación del usuario requiere el aviso con tiempo e información suficiente para permitir la impugnación de la vigilancia.

Dos aspectos resaltan de este Principio. El primero es el derecho a conocer de la restricción del derecho a la privacidad. Los 13 Principios precisan las circunstancias en que puede retrasarse (si bien nunca obviarse) dicha comunicación: cuando la notificación constituye un serio peligro a la finalidad por la cual la vigilancia fue requerida. En todos los casos, la comunicación deberá realizarse tan pronto como el riesgo desaparezca.

Cualquier retraso de la notificación debe ser aprobado por la autoridad judicial competente. Esta salvaguarda busca garantizar que el retraso se justifique y no se extienda más allá de lo estrictamente necesario para proteger una investigación o para proteger a la persona frente a un riesgo inminente a la vida. Las personas afectadas también deberán tener acceso a los materiales presentados en apoyo de la solicitud de autorización de vigilancia.

El deber de notificación ha sido reconocido por el Artículo 7.4 de la Convención Americana, con el propósito de poner a disposición la información y permitir la impugnación de medidas que restrinjan libertades personales. A propósito de una sentencia condenatoria, la Corte Interamericana ha reconocido que la falta de notificación "es en sí misma violatoria del artículo 8 de la Convención" y pone al afectado "en un estado de incertidumbre respecto

de su situación jurídica y torn[a] impracticable el ejercicio del derecho a recurrir del fallo". [25] El mismo criterio debería aplicarse a otras decisiones judiciales que afecten los derechos fundamentales, especialmente cuando el efecto de las éstas sea desconocido por el afectado.

Además del artículo 7.4, el artículo 25 de la Convención Americana, que recoge el derecho a la protección judicial, dispone que toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales. La Corte IDH, en el caso *Mejía Idrovo vs. Ecuador (2011)*[26], entiende a los recursos efectivos de la siguiente forma:

> *En cuanto a la efectividad del recurso, la Corte ha establecido que para que tal recurso efectivo exista, no basta con que esté previsto por la Constitución o la ley o con que sea formalmente admisible, sino que se requiere que sea realmente idóneo para establecer si se ha incurrido en una violación a los derechos humanos y proveer lo necesario para remediarla. No pueden considerarse efectivos aquellos recursos que, por las condiciones generales del país o incluso por las circunstancias particulares de un caso dado, resulten ilusorios.* [27]

La Corte también reiteró en el caso *Ivcher Bronstein vs. Perú, 2001* en qué consiste un recurso efectivo: [28]

> *[L]a inexistencia de un recurso efectivo contra las violaciones a los derechos reconocidos por la Convención constituye una transgresión de la misma por el Estado Parte en el cual semejante situación tenga lugar. En ese sentido debe subrayarse que, para que tal recurso exista, no basta con que esté previsto por la Constitución o la ley o con que sea formalmente admisible, sino que se requiere que sea realmente idóneo para establecer si se ha incurrido en una violación a los derechos humanos y proveer lo necesario para remediarla. No pueden considerarse efectivos aquellos recursos que, por las condiciones generales del país o incluso por las circunstancias particulares de un caso dado, resulten ilusorios.*[29]

Luego, esta norma añade que los Estados Partes se comprometen no solo a garantizar que la autoridad competente prevista por el sistema legal del Estado decidirá sobre los derechos de toda persona que interponga tal recurso, sino a desarrollar las posibilidades de recurso judicial y a garantizar el cumplimiento, por las autoridades competentes, de toda decisión en que se haya estimado procedente el recurso. Como se expresó anteriormente, ante el secretismo imperante en el ejercicio de facultades de vigilancia estatal, la figura del juez se alza como una de suma relevancia.

El Principio de Notificación del Usuario exige al Estado notificar al usuario. Al mismo tiempo, establece que los proveedores de servicios de comunicaciones pueden comunicar a los suscriptores que hayan sido afectados, bien sea voluntariamente o bajo solicitud.

El Informe del Representante Especial del Secretario General para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas, del año 2011, estableció los principios rectores sobre empresas y derechos humanos. El informe recalca que aquellos buscan crear un sistema interrelacionado y dinámico entre medidas de prevención y reparación en el cual el Estado proporciona protección a estos derechos, las empresas se hacen responsables de respetar los derechos humanos como manifestación primordial de la expectativa social que se tiene de aquellas, y finalmente, dar acceso a vías de reparación puesto que no se puede evitar totalmente la comisión de abusos[30]. El Representante Especial precisa que los principios que plantea se basan, entre otros, en "el papel de las empresas como órganos especializados de la sociedad que desempeñan funciones especializadas y que deben cumplir todas las leyes aplicables y respetar los derechos humanos".[31] La importancia del informe fue reconocido por la OEA en su Resolución del 2014 sobre la promoción y protección de los derechos humanos en el ámbito empresarial. Dicha Resolución reconoce la importancia de seguir impulsando la aplicación de los Principios Rectores de Naciones Unidas sobre Empresas y Derechos Humanos y resalta la importancia de avanzar en el tema, invitando a los Estados Miembros a tenerlos en cuenta en las instancias correspondientes.[32]

El rol de las empresas de telecomunicaciones y de tecnología en caso de percibir un intento de interceptación en las comunicaciones privadas sostenidas por sus usuarios es primordial. Estas empresas, al igual que el Estado y que las personas, están obligadas a respetar los derechos fundamentales, sobre todo cuando por las características propias de la prestación que ofrecen, sólo ellas pueden conocer las vulneraciones llevadas a cabo y detener intromisiones indebidas. En relación a lo anterior, el principio 13.b de los Principios Rectores sobre las empresas y los derechos humanos, establece que:

> *"La responsabilidad de respetar los derechos humanos exige que las empresas:*
>
> *b) Traten de prevenir o mitigar las consecuencias negativas sobre los derechos humanos directamente relacionadas con operaciones, productos o servicios prestados por sus relaciones comerciales, incluso cuando no hayan contribuido a generarlos".*[33]

John Ruggie, al comentar el sentido y alcance de esta disposición, especificó que:

> *"Las empresas pueden estar implicadas en las consecuencias negativas sobre los derechos humanos a través de sus propias actividades o como resultado de sus relaciones comerciales con otras partes. El Principio Rector 19 abunda*

en el tipo de respuestas que deben aportar las empresas a estas situaciones. Desde la perspectiva de estos Principios Rectores, las "actividades" de una empresa incluyen tanto sus acciones como sus omisiones; y sus "relaciones comerciales" abarcan las relaciones con socios comerciales, entidades de su cadena de valor y cualquier otra entidad no estatal o estatal directamente relacionada con sus operaciones comerciales, productos o servicio".[34]

Específicamente, el Dictamen 04/2014 sobre la vigilancia de las comunicaciones electrónicas a efectos de inteligencia y seguridad nacional adoptado por el grupo de protección de datos de la Comisión Europea señala su conformidad con el proyecto de ley del Consejo y Parlamento Europeo de ley sobre protección de datos, en el cual se propone notificar de forma obligatoria a las personas cuando se haya permitido el acceso a sus datos por parte de una autoridad pública en los últimos doce meses, lo cual, según este grupo de trabajo, aumentará la confianza de la población.[35]

IX.

Transparencia

Los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades. 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.

Los Estados deben proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la Vigilancia de las Comunicaciones. Los Estados no deberían interferir con los proveedores de servicios en sus esfuerzos para publicar los procedimientos que aplican en la evaluación y el cumplimiento de solicitudes de los Estados para la Vigilancia de Comunicaciones, se adhieran a esos procedimientos, y publicar los registros de las solicitudes de los Estados para la Vigilancia de las Comunicaciones.

El principio de transparencia exige información pública sobre las reglas y la aplicación de la actividad de vigilancia estatal de comunicaciones, así como el deber de publicar reportes periódicos y detallados con tal información. Además, requiere que los Estados no interfieran con la entrega de información por parte de los proveedores de servicios de comunicaciones. De esta forma, el público en general será capaz de evaluar el contenido y el funcionamiento de las leyes que regulan la vigilancia y de las que garantizan los derechos afectados por ella.

Este Principio encuentra su fundamento en el derecho a acceder a información, reconocido en el Artículo 13.1 de la Convención Americana.

A pesar de que el derecho a buscar, recibir y difundir información se encuentra contenido dentro del derecho a la libertad de expresión, el derecho a la información pública ha sido desarrollado de manera separada e independiente por la jurisprudencia de la Corte Interamericana de Derechos Humanos, al punto de convertirse en el primer tribunal internacional que se refiere de forma específica al derecho a la información como un derecho humano autónomo, garantizado convencionalmente. Al respecto, ha sostenido:

[E]l artículo 13 de la Convención, al estipular expresamente los derechos a

> *"buscar" y a "recibir" "informaciones", protege el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención. Consecuentemente, dicho artículo ampara el derecho de las personas a recibir dicha información y la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información o reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso a la misma para el caso concreto. Dicha información debe ser entregada sin necesidad de acreditar un interés directo para su obtención o una afectación personal, salvo en los casos en que se aplique una legítima restricción. Su entrega a una persona puede permitir a su vez que ésta circule en la sociedad de manera que pueda conocerla, acceder a ella y valorarla.*[36]

Cabe destacar de la cita anterior el establecimiento de la "obligación positiva del Estado" de proveer la información. No se trata solamente de responder a los requerimientos de información, sino de su provisión incluso de oficio. Al respecto, para la Corte "en una sociedad democrática es indispensable que las autoridades estatales se rijan por el principio de máxima divulgación, el cual establece la presunción de que toda información es accesible, sujeto a un sistema restringido de excepciones".[37] La Corte Interamericana hace así eco de la Declaración Conjunta de 2004 de los relatores para la libertad de expresión de la ONU, la OEA y la OSCE, en la que indicaron que "[l]as autoridades públicas deberán tener la obligación de publicar de forma dinámica, incluso en la ausencia de una solicitud, toda una gama de información de interés público", y que "se establecerán sistemas para aumentar, con el tiempo, la cantidad de información sujeta a dicha rutina de divulgación."[38]

El deber de transparencia, como correlato del derecho a la información, goza de especial interés en un régimen democrático. Así lo reconoció la Comisión Interamericana de Derechos Humanos el año 2012 en la publicación "El Derecho de Acceso a la Información en el Marco Jurídico Interamericano", en la cual manifestó que el derecho de acceso a la información pública otorga la información que la ciudadanía necesita conocer para poder participar activamente en la sociedad democrática. Por otro lado, ve la utilidad de este derecho en tanto dicha información sirve no solo para proteger los derechos de los individuos sino para prevenir abusos por parte del Estado. Además, indica que es una herramienta que le brinda a la sociedad civil el poder para luchar contra la corrupción y el secretismo.[39]

El rol protagónico atribuido por los órganos del Sistema Interamericano al derecho de acceso a la información pública aplica plenamente a la vigilancia de las comunicaciones. En efecto, como se dijo, los Estados deben hacer pública la información de interés público, y la vigilancia de las comunicaciones lo es, pues esta transparencia permite saber a las personas de qué manera funcionan los mecanismos que son altamente invasivos y cómo afectan a los

derechos fundamentales. Tal información es clave no sólo para conocer las formas de defensa ante tales intromisiones, sino también para tomar conocimiento de las circunstancias en las cuales sus derechos están siendo vulnerados y así poder ejercer las acciones debidas para poner fin a dicha situación.

Al respecto, los Relatores Especiales de Naciones Unidas y de la Comisión Interamericana de Derechos Humanos de la OEA, en su Declaración Conjunta, afirmaron que las normas legales deben asegurar que el público pueda acceder a información sobre programas de vigilancia, su alcance y controles existentes. Los Relatores establecen la obligación del Estado de diseminar los procesos concernientes a la autorización de medidas de vigilancia, la selección de objetivos, el manejo de los datos, e información sobre el uso de técnicas de vigilancia y su alcance. También instan al Estado a permitir a las empresas proveedoras de servicios informar a sus usuarios sobre los procedimientos que ellos implementan, y a aportar cuando menos, información agregada sobre el número y el alcance de las solicitudes que reciben. Finalmente, los Relatores dejan clara la obligación de los Estados de divulgar ampliamente información sobre programas ilegales de vigilancia.[40] La información concerniente a la vigilancia no deberá ser confidencial o reservada *a priori,* antes de que suceda. Toda clasificación de información debe cumplir con la prueba de daño, como se estipula en el caso *Claude-Reyes y otros vs. Chile:*[41]

> *58 (c)"de acuerdo a los amplios términos del [a]rtículo 13, el derecho al acceso a la información debe estar regido por el 'principio de máxima divulgación'". "[L]a carga de la prueba corresponde al Estado, el cual tiene que demostrar que las limitaciones al acceso a la información son compatibles con las normas interamericanas sobre libertad de expresión". "Ello significa que la restricción no sólo debe relacionarse con uno de [los] objetivos [legítimos que la justifican], sino que también debe demostrarse que la divulgación constituye una amenaza de causar substancial perjuicio a ese objetivo y que el perjuicio al objetivo debe ser mayor que el interés público en disponer de la información" (prueba de proporcionalidad)*

Además, al clasificar la información como confidencial, se debe demostrar que existe un daño probable que afecte el interés general; como consecuencia, sería necesario explicar las razones por las cuales la información no sería revelada. Adicionalmente, el posible daño causado al interés general debe ser mayor que el derecho de las personas a saber por "razones de interés público". Sólo de esta manera podremos distinguir entre la confidencialidad basada en criterios políticos y la confidencialidad basada en cuestiones de interés público. Esto asegurará el respeto por el derecho de acceso a la información.

X.

Supervisión Pública

Los estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones. Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, según proceda, al acceso a información secreta o clasificada para valorar si el Estado está haciendo un uso legítimo de sus funciones legales, para evaluar si el Estado ha publicado de forma transparente y precisa información sobre el uso y alcance de las técnicas y poderes de la Vigilancia de las Comunicaciones; y para formular determinaciones públicas en cuanto a la legalidad de dichas acciones, incluyendo la medida en que cumplan con estos principios. Mecanismos de supervisión independientes deben establecerse, además de cualquier supervisión ya proporcionada a través de otra rama del gobierno.

En una democracia es importante que aquellos funcionarios públicos a quienes se les ha confiado la facultad de llevar a cabo la vigilancia de las comunicaciones de las personas estén sujetos a una supervisión efectiva, con el fin de asegurar que esas facultades sean usadas legítimamente y no de manera arbitraria, y que rindan cuentas ante el público en general.[42]

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, en el estudio especial sobre derecho a acceso a la información elaborado en el año 2006, se refirió a los límites legítimos que pueden argumentarse para delimitar el derecho de acceso a la información pública. En dicha oportunidad, la Comisión reconoció el derecho al acceso a la información siguiendo al artículo 13.1 de la Convención Americana sobre la libertad de pensamiento y opinión, y sostuvo que los derechos o reputación de los demás —incluyendo la seguridad nacional, el orden público y la salud o moral públicas— son límites a este derecho, según el Artículo 13.2.[43]

En ese mismo estudio, se cita a "Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información", los cuales, en sus principios 11 y 12, establecen tanto la regla general sobre acceso a la información como la interpretación de la seguridad nacional como excepción al acceso a la información. Así, se señala que todo individuo tiene el derecho de obtener información de las autoridades públicas, incluso información relativa a la seguridad nacional, y que el gobierno solo puede denegar aquella en caso de que pueda demostrar que la restricción consta en una ley y que es

necesaria para proteger un interés legítimo de seguridad nacional, no pudiendo denegar el acceso de modo terminante, sino que únicamente en las categorías que se designen de forma específica en la legislación que sean necesarias para proteger un interés legítimo de seguridad nacional.[44]

Respecto de esta limitación basada en la seguridad nacional, la Relatoría Especial para la Libertad de Expresión es clara, al señalar que:

> *"las restricciones al derecho de acceso por motivos de seguridad nacional sólo serán válidas cuando estén orientadas a proteger la integridad territorial del país y en situaciones excepcionales de extrema violencia que representen un peligro real e inminente de colapso del orden democrático. Una restricción sobre la base de la seguridad nacional no es legítima si su propósito es proteger los intereses del gobierno y no de la sociedad en su conjunto."*[45]

Como es posible observar, tanto la Comisión Interamericana de Derechos Humanos a través de esta Relatoría Especial para la Libertad de Expresión como los Principios de Johannesburgo establecen como norma general el llamado principio de máxima divulgación, el cual, según Ferreyra (2013), "establece la presunción de que toda información es accesible, sujeto a un sistema restringido de excepciones."[46]

La Corte Interamericana también se ha referido a las excepciones al principio general de máxima divulgación, recogiendo la opinión de la Comisión Interamericana de Derechos Humanos en el sentido de que "cuando se trata de la investigación de un hecho punible, la decisión de calificar como secreta la información y de negar su entrega jamás puede depender exclusivamente de un órgano estatal a cuyos miembros se les atribuye la comisión del hecho ilícito". [47]

En la Declaración Conjunta del 2004 del Relator Especial de las Naciones Unidas para la Libertad de Opinión y Expresión, el Representante de la Organización para la Seguridad y Cooperación en Europa y el Relator Especial de la OEA para la Libertad de Expresión, se afirma que no basta con sólo reconocer el derecho de acceso a la información pública; las autoridades nacionales deben tomar medidas activas para asegurar la superación de la cultura del secretismo, tales como sanciones, campañas de información y sensibilización pública y asignación tanto de recursos como de atención necesaria para lograr una implementación eficaz de este tipo de normativa.[48]

El Principio de Supervisión Pública refleja lo estipulado por los órganos del sistema, en especial, la Comisión Interamericana sobre la importancia de que funcionen apropiadamente los órganos de monitoreo y supervisión.[49]

XI.

Integridad de las comunicaciones y sistemas

> *A fin de garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que poner en peligro la seguridad con fines estatales casi siempre afecta la seguridad en términos generales, los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado. 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.*[50]

El principio de integridad implica tres obligaciones negativas en cabeza del Estado. En primer lugar, prohíbe a los Estados obligar a los proveedores de servicios o de "software" o "hardware" a diseñar o a elaborar tecnologías de comunicación con mecanismos de vigilancia. En segundo lugar, prohíbe a los Estados obligar a los prestadores de servicios a recolectar datos de los usuarios. Y en tercer lugar, prohíbe a los Estados imponer restricciones al anonimato.

Más allá de la consagración del derecho a la privacidad, los tratados internacionales no han hecho referencia a las obligaciones antes mencionadas. No obstante, existe plena coincidencia entre los Principios y la opinión del Relator Especial sobre la libertad de expresión de las Naciones Unidas, quien expresara, lo siguiente:

> *"Los Estados deben abstenerse de obligar al sector privado a aplicar medidas que pongan en riesgo la privacidad, la seguridad y el anonimato de los servicios de comunicaciones, incluidos los que requieren el establecimiento de capacidad de interceptación con fines de vigilancia por el Estado o la prohibición del uso de cifrado.*[51]

Igualmente, tanto la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos como el Relator Especial para la libertad de opinión y expresión de Naciones Unidas han resaltado la importancia del anonimato. El Sistema Interamericano destaca a este como una de las dos políticas concretas mínimas vinculadas al ejercicio del derecho a la libertad de expresión a través de internet (siendo la otra la protección de datos personales)[52] y el Relator Kaye lo define como "el vehículo idóneo

(junto al cifrado) para la seguridad en línea y para proveer al individuo de medios para proteger su privacidad, empoderándolos a navegar, leer, desarrollar y compartir opiniones e información sin interferencias, además de permitir a periodistas, organizaciones de la sociedad civil, miembros de grupos étnicos y religiosos, a quienes sean perseguidos por su identidad de género, activistas, académicos, artistas y a todo quien ejerza sus derechos a la libertad de opinión y expresión."[53]

XII.

Garantías para la cooperación internacional

> *En respuesta a los cambios en los flujos de información y en las tecnologías y servicios de comunicaciones, los Estados pueden necesitar procurar la asistencia de un proveedor de servicios extranjero y otros Estados. En consecuencia, los tratados de asistencia judicial recíproca (MLAT, por sus siglas en inglés) y otros acuerdos celebrados por los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte el estándar disponible con el mayor nivel de protección para las personas.*
>
> *El principio de la doble incriminación debe ser aplicado en el momento en que los Estados procuren asistencia para efectos de hacer cumplir su legislación interna. Los Estados no pueden utilizar los procesos de asistencia judicial recíproca y las solicitudes extranjeras de Información Protegida para saltearse las restricciones del derecho interno relativas a la Vigilancia de las Comunicaciones. Los procesos de asistencia judicial recíproca y otros acuerdos deben estar claramente documentados, a disposición del público y sujetos a las garantías de equidad procesal.*

Los 13 Principios exigen que el estándar más protector de los derechos de las personas se aplique cuando exista cooperación entre varios países, e igualmente exigen respetar el principio de doble incriminación (es decir, que las acciones de una persona deben representar un delito tanto en el Estado requirente como en el requerido) para el ejercicio de facultades de vigilancia en la investigación que involucre a más de un Estado. Asimismo, señalan que asistencia judicial recíproca no puede servir para eludir restricciones internas (por ejemplo, si una agencia de inteligencia recibe información de una entidad extranjera y no de su propia vigilancia). También a la asistencia recíproca se aplican principios de transparencia y debido proceso.

En el sistema interamericano, está plenamente vigente un tratado de asistencia mutua en materia penal entre los miembros de la OEA, en cumplimiento del propósito del Artículo 2. (e) de la Convención Americana. Los Principios establecen nuevos estándares para esa cooperación, exigiendo un nivel de protección más alto que el actualmente existente.

XIII.

Garantías contra el acceso ilegítimo y derecho a recurso efectivo

> *Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los "whistle blowers" y medios de reparación a las personas afectadas. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba derivada de dicha información. Los Estados también deben promulgar leyes que establezcan que, después de que el material obtenido a través de la Vigilancia de las Comunicaciones ha sido utilizado con la finalidad por el que fue obtenida la información, el material no debe ser retenido, en su lugar, debe ser destruido o devuelto a los afectados.*

En primer término, el principio final exige sanción penal y civil, contra la vigilancia ilegal de comunicaciones, tanto por el Estado como por privados, además de mecanismos de reparación. Este principio se ve reflejado tanto en el Artículo 8 de la Declaración Universal de Derechos Humanos, el Artículo 2.3 del Pacto Internacional de Derechos Civiles y Políticos, el Artículo XVIII de la Declaración Americana de los Derechos Humanos, y el Artículo 25 de la Convención Americana sobre Derechos Humanos. En esta última disposición se expresa:

> *"Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales."*

Esta disposición consagra el deber estatal de establecer los respectivos recursos y de asegurar su efectividad. Los Principios van más allá, estableciendo de forma explícita la procedencia de sanciones penales y civiles.

En el sistema interamericano, la obligación del Estado de proveer sanciones y medidas de reparación no está condicionada a la existencia de recursos ejercidos por los posibles

afectados. Para la Corte Interamericana, "los Estados deben prevenir, investigar y sancionar toda violación de los derechos reconocidos por [la Convención Americana] y procurar, además, el restablecimiento, si es posible, del derecho conculcado y, en su caso, la reparación de los daños producidos por la violación de los derechos humanos."[54]

Los 13 Principios incluyen la exigencia de protección a los denunciantes o "whistleblowers" en inglés, a fin de que la revelación de actos ilegales no sea a su vez sujeta a sanción. Esta protección emana del derecho a buscar, recibir y difundir información reconocido en el Artículo 19 de la DUDH, en el Artículo 19.2 del PIDCP, y en el Artículo 13.1 de la Convención Americana, protección en virtud de la cual el acto de alerta, relativo a cuestiones de interés público, es en sí mismo un ejercicio del derecho a la libertad de expresión. La protección de los denunciantes se ha convertido en una cuestión requerida por distintos Relatores Especiales de organismos internacionales.[55] A nivel de tratados, y de forma más específica, el Artículo 33 de la Convención de las Naciones Unidas contra la Corrupción, expresa, en términos optativos para los Estados:

> *"Cada Estado Parte considerará la posibilidad de incorporar en su ordenamiento jurídico interno medidas apropiadas para proporcionar protección contra todo trato injustificado a las personas que denuncien ante las autoridades competentes, de buena fe y con motivos razonables, cualesquiera hechos relacionados con delitos tipificados con arreglo a la presente Convención."*

Los 13 Principios exigen también que la información obtenida en contravención a los principios sea inadmisible como prueba contra los afectados, directa o indirectamente, en tanto se trataría de una prueba obtenida en desconocimiento del derecho a la privacidad. En este punto, los 13 Principios recogen aspectos del debido proceso desarrollados como reglas en legislaciones nacionales y subyacentes al debido proceso en los términos ya descritos. Los 13 Principios exigen también la devolución o destrucción del material obtenido mediante vigilancia de comunicaciones una vez concluida su utilidad, recogiendo también reglas como las existentes para la cancelación o eliminación de datos personales. En este punto, los Principios elevan esas reglas a un estándar propio del carácter de derecho fundamental que puede afectarse por la recolección, conservación o procesamiento de esa información.

Recomendaciones

Solicitamos que la Comisión Interamericana de Derechos Humanos (CIDH) se ocupe de estudiar la aplicación de los derechos humanos a la vigilancia de las comunicaciones. Para tal fin, los Principios son una guía útil.

En particular, recomendamos que el informe de la CIDH aborde el estudio de los siguientes temas de interés:

- El derecho a la privacidad como un derecho universal, cuyo disfrute no depende de la nacionalidad o la ubicación de una persona, ni que puede ser reconocido y protegido de manera discriminatoria.

- El reconocimiento explícito de que cualquier acto de vigilancia de las comunicaciones—incluidas la recolección, monitoreo, interceptación, control, retención, adquisición, o toma de custodia de las comunicaciones—supone una injerencia en las libertades fundamentales, que debe ser justificada con arreglo al derecho internacional de los derechos humanos. Es decir que toda limitación permisible debe cumplir—al menos—con los principios de legalidad, objetivo legítimo, idoneidad, necesidad, proporcionalidad y debido proceso;

- El reconocimiento de la obligación de los Estados de respetar y garantizar los derechos humanos de las personas, asegurando que los procedimientos legales que rijan cualquier interferencia con las libertades fundamentales estén enumerados apropiadamente en la ley, sean practicados coherentemente y estén disponibles para el público general, en conformidad con las restricciones permitidas por la Convención;

- La afirmación de que la vigilancia masiva (o "recolección de información a granel") que implique la retención o recolección de datos a priori de una parte importante (o particularmente vulnerable) de la población es una injerencia inherentemente desproporcionada en las libertades civiles;

- La necesidad de hacer más transparente el uso y el alcance de las leyes de vigilancia de las comunicaciones, y de los reglamentos, actividades y poderes que las desarrollan;

- La necesidad de notificar a los afectados acerca de cualquier tipo de vigilancia, así como también de brindarles la oportunidad para obtener un debido proceso y recursos para subsanar la vigilancia indebida.

- La necesidad de establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas en la vigilancia de las

comunicaciones;

- La necesidad de que los Estados provean suficiente protección a los informantes ("whistleblowers") que revelen violaciones a los derechos humanos, así como medios de reparación a las personas afectadas por la vigilancia de las comunicaciones;

- La reiteración de que las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente.

- La importancia de reiterar que las personas tienen el derecho a expresarse anónimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios, ya sea de manera directa o mediante tareas para afectar la integridad de los sistemas de comunicaciones o de los servicios ofrecidos por los proveedores.

- La necesidad de que los Estados procuren que las empresas de comunicaciones que prestan servicios bajo su jurisdicción puedan honrar sus obligaciones de derechos humanos, asegurando que los mecanismos para las solicitudes de información transnacionales realizadas por el Estado cumplan con los estándares exigidos por el derecho internacional.

1 OC-6/86 de 1986, conclusión.

2 Corte IDH. La Expresión "Leyes" en el Artículo 30 de la Convención Americana sobre Derechos Humanos. Opinión Consultiva OC-6/86 de 1986, párr. 18.

3 Caso Escher y otros vs. Brasil.

4 David Kaye, Informe del Relator Especial del Consejo de Derechos Humanos sobre el uso del cifrado y anonimato para ejercer los derechos a la libertad de opinión y de expresión en la era digital, A/HRC/29/32, 2015, disponible en: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx

5 Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, párr. 12, disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

6 OC-6/86 de 1986,párr. 29.

7 Corte IDH. La Colegiación Obligatoria de Periodistas (Arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85,párr.67.

8 Convención Interamericana contra toda forma de discriminación e intolerancia (A-69), disponible en: http://www.oas.org/en/sla/dil/inter_american_treaties_A-69_discrimination_intolerance.asp

9 Corte IDH, *Tristán Donoso vs. Panamá*, párr. 56; Corte IDH, *Escher y otros vs. Brasil*, párr. 116.

10 Así, por ejemplo, a propósito del derecho a la libre circulación, el Comité de Derechos Humanos de Naciones Unidas, Observación General no. 27, 1999, CCPR/C/21/Rev.1/Add.9, párr. 14. Se hace explícita la conveniencia de extender tal interpretación a las restricciones al Artículo 17 del PIDCP; cfr. Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, A/HRC/13/37, párr. 18.

11 Corte IDH, *Fontevecchia y D'Amico v. Argentina*, párr. 53.

12 Corte IDH, *Tristán Donoso vs. Panamá*, párr. 56; Corte IDH, *Escher y otros vs. Brasil*, párr. 116.

13 Corte IDH, Chaparro Álvarez y Lapo Íñiguez vs Ecuador, párrafo 93.

14 Corte IDH, *Kimel vs Argentina*, párrafo 83 citado en Defensoría del Pueblo de la República de Panamá. "*Jurisprudencia de la Corte Interamericana de Derechos Humanos en Materia de Protección de la Honra y de la Libertad de Expresión*". En línea, disponible en: http://defensoria.gob.pa/libros/25.pdf [Fecha de consulta: 16 de diciembre de 2015], p. 16.

15 Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, A/HRC/13/37, párr. 17 y 18.

16 OC-5/85, párr. 46.

17 Corte IDH, *Baena Ricardo y otros vs. Panamá*. Competencia, párr. 79; *Mohamed vs. Argentina*, párr. 83.

18 Corte IDH. *Apitz Barbera y otros ("Corte Primera de lo Contencioso Administrativo") vs. Venezuela*, párr. 55.

19 Corte IDH. *Apitz Barbera y otros ("Corte Primera de lo Contencioso Administrativo") vs. Venezuela*, párr. 56.

20 Corte IDH, *Escher vs. Brasil*, párr. 139

21 Blanco, C y Salmón, E. 2012. "*El Derecho al Debido Proceso en la Jurisprudencia de la Corte Interamericana de Derechos Humanos*" Disponible en línea en: http://idehpucp.pucp.edu.pe/images/publicaciones/derecho_al_debido_proceso_en_jurisprudencia_de_corte_interamericana_ddhh.pdf [Fecha de consulta: 17 de diciembre de 2015], p. 241.

22 Blanco, C y Salmón, E. 2012. "*El Derecho al Debido Proceso en la Jurisprudencia de la Corte Interamericana de Derechos Humanos*". En línea, disponible en: http://idehpucp.pucp.edu.pe/images/publicaciones/derecho_al_debido_proceso_en_jurisprudencia_de_corte_interamericana_ddhh.pdf [Fecha de consulta: 17 de diciembre de 2015], p.241.

23 Los 13 Principios y Análisis Jurídico Internacional de Apoyo y Antecedentes, p. 33.

24 Corte IDH. *Castillo Petruzzi vs. Perú*, párr. 204.

25 Corte IDH, *Vélez Loor Vs. Panamá*, párr. 180.

26 Corte IDH, *Mejía Idrovo vs Ecuador*, 2011, disponible en:http://www.corteidh.or.cr/docs/casos/articulos/seriec_228_ing.pdf

27 Corte IDH, Caso *Velásquez Rodríguez v. Honduras*. Excepciones Preliminares, párr. 93; Caso *comunidad indígena Xákmok Kásek v. Paraguay*. Fondos, Reparaciones y Costas. Sentencia del 24 de agosto de 2010. Serie C No. 214, párr. 140, y Caso *Abrill Alosilla y otros vs. Perú*, supra nota 19, párr. 75.

28 Corte IDH, *Ivcher-Bronstein vs. Perú*. Sentencia del 6 de febrero de 2001 (Fondos, Reparaciones y Costas) Párrafo 136, disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_74_ing.pdf

29 Caso de la Corte Constitucional, Sentencia del 31 de enero de 2001, Corte IDH. (Ser. C) No. 71 (2001), párrafo 89, y Garantías Judiciales en Estados de Emergencia (Artículos 27(2), 25 y 8, Convención Americana sobre Derechos Humanos.

30 Naciones Unidas, Asamblea General, Consejo de Derechos Humanos. 2011. Informe del Representante Especial del Secretario General para la Cuestión de los Derechos Humanos y las Empresas Transnacionales y Otras Empresas, John Ruggie, Principios Rectores sobre las empresas y los derechos humanos, p. 4.

31 Ibíd., p.7.

32 AG/RES. 2840 (XLIV-O/14) promoción y protección de los derechos humanos en el ámbito empresarial, aprobada en la segunda sesión plenaria celebrada el 4 de junio de 2014, disponible en: https://www.oas.org/es/sla/ddi/docs/AG-RES_2840_XLIV-O-14.pdf

33 Naciones Unidas, Asamblea General, Consejo de Derechos Humanos. 2011. Informe del Representante Especial del Secretario General para la Cuestión de los Derechos Humanos y las Empresas Transnacionales y Otras Empresas, John Ruggie, Principios Rectores sobre las empresas y los derechos humanos p. 16.

34 Naciones Unidas, Asamblea General, Consejo de Derechos Humanos. 2011. Informe del Representante Especial del Secretario General para la Cuestión de los Derechos Humanos y las Empresas Transnacionales y Otras Empresas, John Ruggie, Principios Rectores sobre las empresas y los derechos humanos p. 16.

35 Grupo de Trabajo del artículo 29, Opinión 04/2014 sobre vigilancia de las comunicaciones electrónicas para propósitos de inteligencia y seguridad nacional, 10 de abril de 2014, WP215, p. 15.

36 Corte IDH, *Claude Reyes y otros vs. Chile*, párr. 77.

37 Corte IDH, *Claude Reyes y otros vs. Chile*, párr. 92.

38 Declaración Conjunta de los Relatores de Libertad de Expresión de la ONU, la OEA y la OSCE de 6 de diciembre de 2004. Disponible en: http://www.cidh.org/relatoria/showarticle.asp?artID=319&lID=2

39 OEA, Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. 2012. "El Derecho de Acceso a la Información en el Marco Jurídico Interamericano" Segunda Edición. En línea, disponible en https://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%202012%202da%20edicion.pdf [Fecha de consulta: 23 de diciembre de 2015], p. 10.

40 Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, párrafo 12

41 Corte IDH. Caso *Claude-Reyes y otros. v. Chile*, Sentencia del 19 de septiembre de 2006 (Fondos, Reparaciones y Costas)

42 *Véase* también los *Principios de Tshwane sobre Seguridad Nacional y el Derecho a la Información* para una discusión de la autoridad del Estado de retener información del público por razones de seguridad nacional. Disponible en http://www.right2info.org/national-security/Tshwane_Principles.

43 OEA, Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. 2006. "Estudio Especial Sobre el Derecho de Acceso a la Información". En línea, disponible en: http://cidh.oas.org/relatoria/section/Estudio%20Especial%20sobre%20el%20derecho%20de%20Acceso%20a%20la%20Informacion.pdf [Fecha de consulta: 21 de diciembre de 2015], p. 48.

44 Article 19. 1996. Los Principios de Johannesburgo Sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información. En línea, disponible en: https://www.article19.org/data/files/medialibrary/1803/Johannesburg-Principles.Spa.pdf [Fecha de consulta: 21 de diciembre de 2015], p. 15.

45 OEA, Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. 2006. op. cit., loc. cit.

46 Ferreyra, Leandro. 2013. "Acceso a la Información: Hacia la Democratización de la Administración Pública". Lecciones y Ensayos 91, p. 123.

47 Corte IDH, *Myrna Mack Chang Vs. Guatemala.* Fondo, Reparaciones y Costas, párr. 181; Corte IDH, *Claude Reyes y otros vs. Chile*, párr. 202. Cfr. Comisión Interamericana de Derechos Humanos, *Tercer Informe sobre la Situación de los derechos humanos en Colombia*, OEA/Sev.L/V/II.102, Doc. 9 rev. 1, párr. 59.

48 OEA. 2004. Mecanismos Internacionales para la Promoción de la Libertad de Expresión. En línea, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=319&lID=2 [Fecha de consulta: 22 de diciembre de 2015].

49 *Véase* por ejemplo, el Grupo de Trabajo del artículo 29, Opinión 04/2014 sobre vigilancia de las comunicaciones electrónicas para propósitos de inteligencia y seguridad nacional, 10 de abril de 2014, WP215. Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opi....

50 Informe del Relator Especial de Naciones Unidas sobre la protección y promoción del derecho a la libertad de opinión y expresión, Frank La Rue, 16 Mayo 2011, A/HRC/17/27, para 84.

51 Informe del Relator Especial para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión (A.HRC/23/40), párr. 96.

52 Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. 2013. Libertad de Expresión e Internet, p. 63.

53 Informe del Relator Especial para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, David Kaye (A/HRC/29/32), p. 3. La traducción del texto original en inglés es nuestra.

54 Corte IDH. *Velásquez Rodríguez vs. Honduras.* Fondo, párr. 166.

55 Informe del Relator Especial para la Promoción y Protección del Derecho a la Opinión y Expresión, Abid Hussain, 8 de enero de 2000; Declaración Conjunta del Relator Especial de las Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y Expresión y la Relatora Especial de la Comisión Interamericana de Derechos Humanos para la Libertad de Expresión de la, 21 de junio de 2013; Informe del Relator Especial para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, Martin Scheinin, A/HRC/10/3, 4 de febrero de 2009, párr. 61.