NECESARIOS & PROPORCIONADOS

PRINCIPIOS INTERNACIONALES SOBRE LA APLICACIÓN DE LOS DERECHOS HUMANOS A LA VIGILANCIA DE LAS COMUNICACIONES

Créditos

Los Principios Internacionales de Derechos Humanos sobre Vigilancia de las Comunicaciones fue escrito colaborativamente por organizaciones de privacidad y activistas de todo el mundo, incluyendo **Access, Article 19, Asociación Civil por la Igualdad y la Justicia, Asociaciónpor los DerechosCiviles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India, Comision Colombiana de Juristas, Electronic Frontier Foundation, European Digital Rights, Fundación Karisma, Fundación Vía Libre, Open Net Korea, Open Rights Group, Privacy International**, *y el* **Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.** Además, participaron en su discusión los asistentes a la reunión de Bruselas organizada **por Privacy International,** la reunión de **Brazil organizada** por EFF asi como todos aquellos expertos que enviaron sus comentarios **a través de la convocatoria en línea realizada**. Organizaciones como **IP Justice, IFEX Network, SHARE Foundation - SHARE Defense** *e* **Instituto NUPEF** colaboraron conectando grupos en distintas partes del mundo.

For more information, visit

necessaryandproportionate.org/text

Antecedentes

El proceso de elaboración de estos Principios se inició en octubre de 2012 en una reunión de más de 40 expertos de seguridad y privacidad en Bruselas. Después de una amplia consulta inicial, que incluyó una segunda reunión en Río de Janeiro en diciembre de 2012, Access, FEP y Privacy International condujeron un proceso de redacción colaborativa inspirada en la pericias obre derechos humanos y derechos digitales de expertos de todo el mundo. La primera versión de los Principios se finalizó el 10 de julio de 2013, y fue lanzada oficialmente en el Consejo de Derechos Humanos de la ONU en Ginebra en septiembre de 2013. El éxito rotundo y la adopción global de los Principios por más de 400 organizaciones en todo el mundo hizo necesario un serie de cambios concretos en el lenguaje del texto, fundamentalmente superficiales a fin de asegurar su interpretación uniforme y la aplicación en todas las jurisdicciones. De marzo a mayo de 2013, otra consulta se llevó a cabo para determinar y corregir esos problemas textuales y actualización de los Principios en consecuencia. El efecto y la intención de los Principios no se alteró por estos cambios.Esta versiónes el producto final de estos procesos y es la versión autorizada de los Principios.

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

VERSIÓN FINAL 10 DE MAYO DE 2014

A medida que avanzan las tecnologías que facilitan la vigilancia estatal de las comunicaciones, los Estados están fallando en garantizar que las leyes, normas, actividades, poderes y autoridades relacionadas con la Vigilancia de las Comunicaciones se adhieran a las normas y estándares internacionales de derechos humanos. Este documento intenta clarificar cómo se aplica el derecho internacional de los derechos humanos en el actual entorno digital, en particular a la luz del aumento y de los cambios que están teniendo las tecnologías y técnicas de Vigilancia de las Comunicaciones. Estos principios pueden proporcionar a los grupos de la sociedad civil, a la industria y a los Estados un marco para evaluar si las leyes y prácticas de vigilancia, actuales o propuestas, están en línea con los derechos humanos.

Estos principios son el resultado de una consulta global con grupos de la sociedad civil, con la industria y expertos internacionales en legislación sobre Vigilancia de las Comunicaciones, políticas públicas y tecnología.

PREÁMBULO

La intimidad es un derecho humano fundamental y es cardinal para el mantenimiento de sociedades democráticas. Es esencial a la dignidad humana y refuerza otros derechos, tales como la libertad de expresión y de información, y la libertad de asociación. Además, es reconocida por el derecho internacional de los derechos humanos.[1]

La Vigilancia de las Comunicaciones interfiere con el derecho a la intimidad entre varios otros derechos humanos. Como resultado, sólo puede estar justificada cuando es prescrita por ley, es necesaria para lograr un objetivo legítimo, y es proporcional al objetivo perseguido.[2]

Antes de la adopción pública de Internet, principios jurídicos bien definidos y cargas logísticas inherentes al monitoreo de las comunicaciones crearon límites a la Vigilancia de las Comunicaciones por el Estado. En décadas recientes, esas barreras logísticas a la vigilancia han disminuido y ha perdido claridad la aplicación de principios jurídicos en los nuevos contextos tecnológicos. La explosión del contenido digital en las comunicaciones y de la información acerca de ellas e—información sobre las comunicaciones o el uso de dispositivos electrónicos de una persona—el costo cada vez menor de almacenamiento y la minería de grandes cantidades de datos, y el suministro de contenido personal a través de proveedores de servicios externos, hacen posible llevar la Vigilancia de las Comunicaciones estatal a una escala sin precedentes.[3]

Mientras tanto, las conceptualizaciones de la legislación vigente en materia de derechos humanos no ha seguido el ritmo

de las modernas y cambiantes tecnologías y técnicas estatales de Vigilancia de Comunicaciones, la habilidad del Estado para combinar y organizar la información obtenida mediante distintas técnicas y tecnologías de vigilancia, o la creciente susceptibilidad de la información a la que se puede acceder.

La frecuencia con la que los Estados procuran acceder tanto al contenido de las comunicaciones como a los metadatos de las comunicaciones aumenta drásticamente, sin controles adecuados.[4]

Los metadatos de las comunicaciones pueden crear un perfil de la vida de un individuo, incluyendo condiciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tan o, incluso, más detalladamente de lo que sería posible desde el contenido de las comunicaciones[5] A pesar del gran potencial para la intromisión en vida de el individuo y el efecto negativo sobre las asociaciones políticas y otras, las leyes, normas, poderes o autoridades a menudo ofrecen a los metadatos de las comunicaciones un menor nivel de protección y no ponen restricciones suficientes sobre cómo pueden ser posteriormente utilizado por los Estados.

ÁMBITO DE APLICACIÓN

Los Principios y el Preámbulo son holísticos y autorreferenciales; cada principio y el preámbulo deberán leerse e interpretarse como parte de un marco más amplio que, en conjunto, logran una única meta: garantizar que las leyes, políticas y prácticas relacionadas con las Vigilancia de las Comunicaciones se adhieren a las leyes y estándares internacionales de derechos humanos y protegen adecuadamente los derechos humanos individuales como la privacidad y la libertad de expresión. Así, con el fin de que los Estados cumplan efectivamente sus obligaciones dimanantes de la legislación internacional sobre derechos humanos en lo relativo con la Vigilancia de las Comunicaciones, deben cumplir con los principios que se presentan a continuación.

Éstos se aplican a la vigilancia llevada a cabo dentro de las fronteras de un Estado o extraterritorialmente. Los principios también se ponen en práctica con independencia de la finalidad de la vigilancia, incluyendo la aplicación de la ley, la protección de la seguridad nacional, la recopilación de inteligencia, u otra función gubernamental. También se emplean en relación con la obligación del Estado de respetar y garantizar los derechos individuales, así como al deber de proteger los derechos de las personas ante abusos por parte de actores no estatales, incluida la Empresas Comerciales.[6]

Las Empresas Comerciales tienen la responsabilidad de respetar la privacidad individual y otros derechos humanos, en particular dado el papel fundamental que desempeñan en el diseño, desarrollo y difusión de tecnologías.; permitir y proporcionar comunicaciones; y en la facilitación de determinadas actividades de vigilancia del Estado.[7] Sin embargo, estos principios articulan los deberes y obligaciones de los Estados cuando se involucran en la Vigilancia de Comunicaciones.

CAMBIO DE TECNOLOGÍA Y DEFINICIONES

"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.

NECESARIOS & PROPORCIONADOS

Tradicionalmente, el carácter invasivo de la Vigilancia de las Comunicaciones ha sido evaluado sobre la base de categorías artificiales y formalistas. Los marcos legales existentes distinguen entre "contenido" o "no contenido", "información del suscriptor" o "metadatos", datos almacenados o datos en tránsito, datos que se tienen en el hogar o en la posesión de un tercero proveedor de servicios.[7]

Sin embargo, estas distinciones ya no son apropiadas para medir el grado de intromisión que la Vigilancia de las Comunicaciones realiza en la vida privada y las relaciones de las personas. Aunque desde hace tiempo se ha acordado que el contenido de la comunicación merece una protección significativa en la ley debido a su capacidad de revelar información sensible, ahora está claro que existe otra información que surge de las comunicaciones, y datos que no son contenido, que puede revelar incluso más acerca de una persona que el contenido en sí, y por lo tanto merece una protección equivalente. Hoy en día, cada uno de estos tipos de información, por sí sola o analizada colectivamente, puede revelar la identidad de una persona, su comportamiento, sus asociaciones, sus condiciones físicas o estado de salud, su raza, color, orientación sexual, origen nacional o puntos de vista, o puede permitir el mapeo de la ubicación de la persona, sus movimientos e interacciones en el tiempo[8], o puede hacer esto respecto de todas las personas en una ubicación determinada, incluyendo una manifestación pública u otro acontecimiento político.

Como resultado, toda la Información Protegida debe recibir la máxima protección de la ley.

Al evaluar el carácter invasivo de la Vigilancia de las Comunicaciones por el Estado, es necesario considerar la potencialidad de la vigilancia de revelar Información Protegida, así como la finalidad para la que el Estado procura la información. Cualquier Vigilancia de las Comunicaciones que posiblemente de lugar

a revelar Información Protegida que pueda poner a una persona en riesgo de ser investigada, de sufrir discriminación o de violación de sus derechos humanos, constituirá una infracción grave a su derecho a la privacidad, y también afectará negativamente el disfrute de otros derechos fundamentales, incluyendo las libertades de expresión, de asociación y de participación política. Ello es así porque estos derechos requieren que las personas sean capaces de comunicarse libres del efecto amedrentador de la vigilancia gubernamental. Será pues necesario en cada caso específico determinar tanto el carácter como los posibles usos de la información que se procura.

Al adoptar una nueva técnica de Vigilancia de las Comunicaciones o ampliar el alcance de una existente, el Estado debe determinar, antes de buscarla, si la información que podría ser adquirida cae en el ámbito de la "Información Protegida", y debería someterse a escrutinio judicial u otro mecanismo de control democrático. La forma de la vigilancia, así como su alcance y duración, son factores relevantes para determinar si la información obtenida a través de la Vigilancia de las Comunicaciones alcanza el nivel de "Información Protegida". Puesto que el monitoreo generalizado o sistemático tiene la capacidad de revelar información privada que excede en mucho la suma de valor informativo de los elementos individuales recogidos, puede elevar la vigilancia de información no protegida a un nivel invasivo que exija una mayor protección.[9]

Determinar si el Estado puede llevar a cabo vigilancia de comunicaciones que interfiera con Información Protegida debe ser compatible con los siguientes principios:

LOS 13 PRINCIPIOS

LOS 13 PRINCIPIOS

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 estandar 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.

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.

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.

Idoneidad

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

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, debe demostrar lo siguiente-a una autoridad judicial competente-antes de la realización de la Vigilancia de las Comunicaciones para los fines de hacer cumplir la ley, la protección de la seguridad nacional, o la recolección de inteligencia:

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

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

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

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

6. La información será accesada solo por la autoridad especifica 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.

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.

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,[10] 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.

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 debe tener la libertad de notificar a las personas de la Vigilancia de las Comunicaciones, de forma voluntaria o bajo petición.

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.

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.[11]

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.

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.[12]

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 la estandar 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 burlar 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.

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.

* El proceso de elaboración de estos Principios se inició en octubre de 2012 en una reunión de más de 40 expertos de seguridad y privacidad en Bruselas. Después de una amplia consulta inicial, que incluyó una segunda reunión en Río de Janeiro en Diciembre de 2012, Access, EFFy Privacy International condujeron un proceso de redacción colaborativa inspirada en la pericia sobre derechos humanos y derechos digitales de expertos de todo el mundo. La primera versión de los Principios se finalizó el 10 de julio de 2013, y fue lanzada oficialmente en el Consejo de Derechos Humanos de la ONU en Ginebra en Septiembre de 2013. El éxito rotundo y la adopción global de los Principios por más de 400 organizaciones en todo el mundo hizo necesario un serie de cambios concretos en el lenguaje del texto, fundamentalmente superficiales a fin de asegurar su interpretación

uniforme y la aplicación en todas las jurisdicciones. De marzo a mayo de 2013, otra consulta se llevó a cabo para determinar y corregir esos problemas textuales y actualización de los Principios en consecuencia. El efecto y la intención de los Principios no se alteró por estos cambios. Esta versión es el producto final de estos procesos y es la versión autorizada de los Principios.

NOTAS AL FIN

1 Declaración Universal de Derechos Humanos, Artículo 12, Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares, Artículo 14, Convención sobre los Derechos del Niño de Naciones Unidas, Artículo 16, Pacto Internacional de Derechos Civiles y Políticos Artículo 17; convenciones regionales incluido Artículo 10 Del Capítulo Africano Carta sobre los Derechos y el Bienestar del Niño, Artículo 11 de la Convención Americana de Derechos Humanos, Artículo 4 de los principios de la Unión Africana sobre la Libertad de Expresión, Artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre, Artículo 21 de la Declaración Derechos Humanos de la ASEAN, Artículo 21 de la Carta Árabe de Derechos Humanos, y Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; Principios de Johannesburgo sobre la Seguridad Nacional, Expresión y Acceso a la Información, Principios de Camden para la Libertad de Expresión y la Igualdad Libre.

2 Declaración Universal de Derechos Humanos, Artículo 29; Comentarios Generales No. 27, Adoptado por el Comité de Derechos Humanos bajo el Artículo 40, Parágrafo 4 del Pacto Internacional de Derechos Civiles y Políticos, CCPR/C/21/Rev.1/Add.9, Noviembre 2, 1999; Ver también Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34, Ver también Frank La Rue; "Informe del Relator Especial del Consejo de Derechos Humanos sobre las implicaciones de la Vigilancia de las Comunicaciones de los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y de expresión", 2013, A.HRC. 23.40 ES.

3 Los metadatos de las comunicaciones pueden incluir información acerca de nuestras identidades (información del abonado, información del dispositivo), las interacciones (origen y destino de las comunicaciones, especialmente las que muestran los sitios web visitados, los libros y otros materiales de lectura, las personas interactuaron con los amigos, familia, conocidos, búsquedas realizadas, los recursos utilizados) y ubicación (lugares y tiempos, proximidades a otros), en suma, los metadatos proporciona una ventana a casi todas las acciones en la vida moderna, nuestros estados mentales, los intereses, las intenciones y los pensamientos más íntimos.

4 Por ejemplo, solamente en el Reino Unido existe aproximadamente 500.000 solicitudes de acceso a los metadatos de las comunicaciones todos los años,

actualmente bajo un régimen de auto-autorización, los servicios policiales puedan autorizar la solicitud de acceso a la información en poder de los proveedores de servicios. Mientras tanto, los datos proporcionados por los informes de transparencia de Google muestran que las solicitudes de datos de los usuarios de los EE.UU. aumentaron solamente de 8.888 en 2010 a 12.271 en 2011. En Corea, cada año había alrededor de 6 millones de solicitudes de abonados de información y alrededor de 30 millones de solicitudes de otras formas de metadatos de comunicaciones en el período 2011-2012, casi de todo lo cual se entregó y se ejecuta. Los datos del año 2012 están disponibles en **http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586**

5 Ver la revisión del trabajo de Sandy Petland, 'Reality Mining', en MIT's Technology Review, 2008, disponible en **http://www2.technologyreview.com/article/409598/tr10-reality-mining/** y ver también Alberto Escudero-Pascual y Gus Hosein, 'Questioning lawful access to traffic data', Communications of the ACM, Vólumen 47 Issue 3, Marzo 2004, páginas 77 - 82.

6 Reporte del Relator de Naciones Unidas sobre la Promoción y Protección de la Libertad de Opinión y Expresión, Frank La Rue, 16 de Mayo 2011, disponible en **http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf**

7 "Las personas revelan los números de teléfono que marcan para llamar o enviar mensajes de texto a sus proveedores de celulares, las direcciones URL que visitan y las direcciones de correo electrónico con las que se comunican a sus proveedores de servicios de Internet y los libros, alimentos y medicamentos que compran a los minoristas en línea. . . No imagino que toda la información voluntariamente revelada a algún miembro del público para un propósito limitado carece, por esa única razón, de la protección de la Cuarta Enmienda. "Los Estados Unidos contra Jones, 565 EE.UU. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurrente)."

8 "El seguimiento a corto plazo de los movimientos de una persona en la vía pública concuerda con las expectativas de privacidad", pero "el uso del monitoreo de GPS a largo plazo en las investigaciones de la mayoría de los delitos afecta a las expectativas de la vida privada." Los Estados Unidos contra Jones, 565 EE.UU., 132 S. Ct. 945, 964 (2012) (Alito, J. concurrente).

9 "La vigilancia prolongada revela tipos de información no reveladas por la vigilancia a corto plazo, como que hace una persona repetidamente, lo que no hace, y lo que hace en conjunto. Este tipo de información puede revelar más sobre una persona que lo que revelaría cualquier viaje individual considerado aisladamente. Visitas repetidas a una iglesia, un gimnasio, un bar, o un corredor de apuestas cuentan una historia no revelada en una sola visita, al igual que una ausencia a cualquiera de estos lugares a lo largo de un mes. La secuencia de los movimientos de una persona puede revelar aún más; un solo viaje a la oficina de un ginecólogo dice poco acerca de una mujer, pero

ese viaje seguido, unas semanas después, de una visita a una tienda de artículos para bebé cuenta una historia diferente. * Una persona que sabe todo de los viajes de otros puede deducir si es un visitante semanal a la iglesia, un bebedor recurrente, un habitual en el gimnasio, un marido infiel, un paciente ambulatorio que recibe tratamiento médico, un asociado de individuos o grupos políticos particulares .. y no sólo un hecho determinado acerca de una persona, si no todos esos hechos "EE.UU. v Maynard, 615 F. 3d 544 (. EE.UU., DC Circ, CA) p 562; EE.UU. v Jones, 565 EE.UU. __, (2012), Alito, J., concurriendo. Por otra parte, la información pública puede entrar en el ámbito de la vida privada cuando se recoge y se almacena en archivos en poder de las autoridades de manera sistemática. Todo esto es aún más cierto cuando esa información se refiere al pasado lejano de una persona ... En opinión de la Corte, tal información, cuando se recoge de manera sistemática y se almacena en un archivo en poder de agentes del Estado , está comprendida en el ámbito de la «vida privada» en el sentido del artículo 8 (1) de la Convención ". (Rotaru contra Rumania, [2000] CEDH 28341/95, párrs. 43-44.

10 El término "debido proceso" puede utilizarse de manera intercambiable con "justicia procesal" y "justicia natural" y está bien articulado en el Convenio Europeo de Derechos Humanos del artículo 6(1) y el artículo 8 de la Convención Americana sobre Derechos Humanos.

11 El Comisionado de Interceptación de Comunicaciones del Reino Unido es un ejemplo de un mecanismo de supervisión independiente de ese tipo. El ICO publica un informe que incluye algunos datos agregados pero no proporciona datos suficientes para examinar los tipos de solicitudes, la extensión de cada petición de acceso, el propósito de las solicitudes, y el escrutinio que se aplica a ellos. Ver **http://www.iocco-uk.info/sections.asp?sectionID=2&type=top**

12 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.

NECESARIOS & PROPORCIONADOS

PRINCIPIOS INTERNACIONALES SOBRE LA APLICACIÓN DE LOS DERECHOS HUMANOS A LA VIGILANCIA DE LAS COMUNICACIONES

ANÁLISIS JURÍDICO INTERNACIONAL DE APOYO Y ANTECENDENTES

MAYO 2014

ELECTRONIC FRONTIER FOUNDATION

Electronic Frontier Foundation y Articulo 19 están muy agradecidos a todos los que nos ayudaron con la investigación y redacción de este documento. En particular agradecemos a Douwe Korff, Profesor de Derecho Internacional de los Derechos Humanos, por la preparación de una versión anterior del documento, y a Cidy Cohn, Gabrielle Guillemin, Tamir Israel, Dr. Eric Metcalfe y Katitza Rodríguez por sus posteriores contribuciones. Extendemos unas palabra de agradecimiento especial a Access, Privacy International, Asociación por los Derechos Civiles, Comisión Colombiana de Juristas, Fundación Karisma, Human Rights Information and Documentation System – HURIDOCS, El Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, y Open Net Korea por revisar y compartir recursos bibliográficos. Aunque intentamos promover una amplia consulta, agradeceríamos recibir aportes adicionales de expertos en los derechos africano y de Europa del Este, tanto de organismos nacionales como regionales, que no están representados con tanta fuerza en esta primera versión del documento.

necessaryandproportionate.org/LegalAnalysis

Tabla de Contenidos

Introducción

Vivimos en una era en donde el rápido desarrollo de la economía y las capacidades de vigilancia digital presentan una serie de retos a muchos de nuestros derechos humanos más celebrados:

- ¿Cómo podemos preservar la intimidad, cuando los gobiernos de todo el mundo pueden, frecuentemente, a bajo costo y de manera invisible, recopilar y analizar las interacciones de cada ciudadano—incluso hasta el nivel de sus libretas de direcciones, documentos y conversaciones—con familiares, amigos y compañeros de trabajo?
- ¿Qué puede quedar de la libertad de asociación cuando segundo a segundo las comunicaciones y las ubicaciones físicas de poblaciones enteras son recopiladas y los datos emitidos por los teléfonos móvil son almacenados?
- ¿Cómo puede la verdadera libertad de expresión y opinión persistir cuando cada vez que vemos una noticia provocadora, leemos un documento polémico o navegamos por la obra de un reconocido autor, un registro digital queda y es visto, leído y navegado por máquinas, algoritmos y agentes del Estado?

Sobre todo, ¿cómo se conservarán nuestros derechos humanos en la era digital cuando muchos de nuestros actos cotidianos, actividades políticas y comunicaciones emiten un flujo continuo de información reveladora, frente a pocas restricciones legales o tecnológicas a la vigilancia, recopilación, análisis y uso en nuestra contra por parte del gobierno?

Estas preguntas y continuas preocupaciones derivadas de las técnicas de vigilancia fueron el punto de partida para la

redacción de los Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones, que explica cómo el derecho internacional de los derechos humanos se emplea en el contexto de la vigilancia de las comunicaciones.[1] Los principios están, por tanto, firmemente enraizados en el derecho internacional de los derechos humanos y la jurisprudencia. La más reciente sucesión de revelaciones por Snowden, precisamente, han demostrado hasta qué punto pueden erosionarse los derechos humanos si no se abordan los desafíos generados por las tecnologías.

El propósito principal de lo que se convirtió en los *13 Principios Necesarios y Proporcionados* (en adelante, "los Principios")[2] fue proporcionar a grupos de la sociedad civil, a los Estados, a los tribunales, a los órganos legislativos y reguladores, a la industria y demás un marco para evaluar si las leyes de vigilancia o las prácticas, actuales o futuras, son compatibles con los derechos humanos. En la era post Snowden, ha quedado claro la urgente necesidad de revisar y aprobar leyes y prácticas nacionales de vigilancia con el fin de que cumplan con los Principios y garanticen la protección de la privacidad de manera transfronteriza.

Al mismo tiempo, una de las principales preocupaciones que guían los Principios fue mantener la aplicación de legislaciones actualizadas frente a los últimos desarrollos tecnológico, garantizando que la fortaleces de las protecciones fundamentales creadas a lo largo de muchos años en la era pre-digital. Los cambios tecnológicos no están precisamente abordados en las actuales legislaciones de derechos humanos. Nuestro objetivo fue identificar los principios básicos que sustentan una sólida protección de los derechos humanos en la era digital. Por esta razón, no todos los enfoques que proponemos han sido apoyados formal o explícitamente por los órganos internacionales de protección de los derechos humanos.

Los Principios se han sido firmados por 400 organizaciones y 300 mil personas alrededor del mundo, y apoyado por la

Conferencia Liberal Democrática del Reino Unido, como también por parlamentarios europeos, canadienses y alemanes.[3] Además, los Principios han sido citados en el informe el Grupo de Revisión del Presidente sobre Inteligencia y Tecnologías de las Comunicaciones de los Estados Unidos,[4] el informe de la Comisión Interamericana de Derechos Humanos,[5] entre otros.[6]

En este documento, la *Electronic Frontier Foundation* y *ARTICLE 19* explican el fundamento legal o conceptual de los Principios.[7] Este documento se divide en tres partes. La primera parte se ocupa de las cuestiones relacionadas con el ámbito de aplicación de los Principios. La segunda sección presenta las definiciones y conceptos clave, a saber, el concepto de "información protegida", en contraste con los enfoques categóricos tradicionales sobre la protección de datos y el derecho a la intimidad, además de incluir una definición de "vigilancia de las comunicaciones". La tercera parte explica el fundamento jurídico y conceptual de cada Principio. De esta forma, se comienza estableciendo el marco fundamental de los derechos humanos que sustenta los derechos a la intimidad, a la libertad de expresión y a la libertad de asociación. También se explica el fundamento legal de cada uno de los Principios, con referencia a la jurisprudencia y las opiniones de una serie de organismos y expertos de derechos humanos, como los relatores especiales de la Naciones Unidas. Hacemos un esfuerzo para diferencias las conclusiones que están basadas en normas firmemente establecidas, de aquellas que sugieren nuevas prácticas cimentadas en los principios fundamentales de los derechos humanos.

Alcance:

APLICACIÓN EXTRATERRITORIAL DE LOS TRATADOS DE DERECHOS HUMANOS

Uno de los aspectos más inquietantes de las revelaciones de Snowden fue el alcance de la cooperación y intercambio de información de inteligencia entre la NSA, la Agencia Británica

de Inteligencia (GCHQ, por sus siglas en inglés) y las otras naciones del *Five Eyes* ('Cinco Ojos'), en el que el material reunido bajo el régimen de vigilancia de un país era rápidamente compartido con los otros. Cada uno de los *Five Eyes* (Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda) están estratégicamente situados para espiar gran parte de las comunicaciones en el mundo, ya que el tránsito de información pasa o se almacenan en sus respectivos territorios. Las organismos de inteligencia extranjeros de estas naciones han construido una red de interoperabilidad a nivel técnico y operativo que se extiende por la red global de comunicaciones. Además, existen acuerdos de intercambio de inteligencia entre naciones que no hacen parte de los *Five Eyes*, de modo que, hay una amplia cooperación—sobre todo entre organismos encargados de hacer cumplir la ley—a través de arreglos más formales, incluidos los tratados de asistencia legal mutua (MLAT, por sus siglas en inglés).

La cooperación internacional entre los gobiernos también plantea dudas en cuanto a cómo y cuándo los Estados pueden ser responsables bajo el derecho nacional e internacional por sus actividades de vigilancia, que pueden tener un impacto mucho más allá de sus propias fronteras. Una cuestión es el grado en que los Estados pueden ser "extraterritorialmente" responsables de sus violaciones de derechos humanos en el extranjero, por ejemplo, la vigilancia de las comunicaciones privadas en otros países. Sin embargo, es importante tener en cuenta que la actual tecnología permite a los Estados monitorear una gran cantidad de tráfico internacional dentro de los límites de sus propias fronteras. Por tanto, es cardinal hacer una breve referencia a la cuestión de la jurisdicción bajo el derecho internacional de los derechos humanos y las diferentes formas en que un Estado puede ser considerado responsable de sus actos, incluso cuando los efectos se hacen sentir más allá de sus fronteras.[8] Nuestra discusión del Principio 12, como se detalla más adelante, ofrece un examen a fondo de esta cuestión en el contexto específico de los MLAT.

Surge un problema central cuando se establecen limitaciones territoriales excesivamente estrechos en relación con la protección de los derechos humanos, ya que rápidamente quedan sin sentido cuando se aplica a las altamente integradas redes globales de comunicación. Históricamente, las limitaciones prácticas obstaculizaron la forma en que un gobierno podía operar para acceder clandestinamente a las comunicaciones de individuos de otro país. Cuando esto ocurría, en teoría, los individuos afectados podían recurrir a las protecciones de su Estado de origen, pues, las actividades de vigilancia necesariamente interferían en la soberanía de otro Estado y, por tanto, violaban sus leyes internas. Sin embargo, la naturaleza de las redes digitales, que se basan en el enrutamiento y almacenamiento sin fronteras para su eficiencia y robustez, permiten a los Estados interceptar grandes cantidades de información extranjera desde la comodidad de sus territorios nacionales. Acompañando a esta nueva capacidad técnica, encontramos un cambio de enfoque tras el 11S, que sitúa a todos los personas—en lugar de a los poderes extranjeros y a los Estados—en el centro de los extraordinarios poderes de vigilancia y recursos de los organismos de inteligencia extranjeros. La combinación de estos factores ha dado lugar a una situación en la que, a menudo, el derecho a la intimidad de los extranjeros ha sido invadido significativa y considerablemente por los organismos de inteligencia extranjeros.[9] Por último, considerando que con frecuencia los organismos de inteligencia extranjeros poseen un rango inmenso para espiar las comunicaciones de los extranjeros,[10] el alto grado de integración de las redes de comunicación ha llevado a muchos de estas entidades a hacer un barrido indiscriminado de todos los datos, defendiéndose con el argumento de alta dificultad que entraña distinguir entre las comunicaciones nacionales de las extranjeras.[11]

En resumen, los gobiernos pueden llevar a cabo la vigilancia dentro y fuera de sus propias fronteras. Sin embargo, el marco legal interno de la mayoría de los países, por lo general, otorga mayor protección al derecho a la intimidad de los nacionales

frente a los no nacionales y no residentes. Como resultado, muchos gobiernos se involucran de forma rutinaria en una mayor vigilancia de las comunicaciones internacionales, con muy poco respeto por la intimidad de las comunicaciones, posiblemente baja la errónea creencia de que sus obligaciones legales solo se extienden con respecto a sus propios nacionales o residentes. Más problemático aún parecieran ser los arreglos entre países para intercambiar información de inteligencia con el fin de obtener material de vigilancia en relación con sus propios nacionales, que de otra forma no podrían obtener bajo sus propios ordenamientos jurídicos. Sin embargo, como se explica más adelante, el disfrute de los derechos fundamentales no se limita a los nacionales de un Estado particular, sino que incluye a todos los individuos, independientemente de su nacionalidad o condición de apátrida, como los solicitantes de asilo, los refugiados, los trabajadores migrantes y otras personas que puedan encontrarse en un territorio o están sometidos a la jurisdicción de un Estado.[12] Además, todas las personas son iguales ante la ley y, en consecuencia, tienen derecho, sin discriminación alguna, a igual protección de la ley.[13]

A tenor de ello, el Preámbulo de los Principios, en la sección sobre el Ámbito de Aplicación, expresamente dispone que los Principios "se aplican a la vigilancia llevada a cabo dentro de un Estado o extraterritorialmente". Esto refleja el requisito del derecho internacional de los derechos humanos sobre el deber de los Estados de respetar los derechos de todas las personas sin distinción ni discriminación, ya sea de "cualquier persona dentro de su territorio o jurisdicción" o simplemente "dentro de su jurisdicción" o "sometida a su jurisdicción".[14]

No obstante, es importante tener claro que la obligación de los Estados de respetar los derechos de las personas dentro de su "jurisdicción" no se limita a los derechos de las personas físicamente en su territorio. En el caso de *Bósforo v. Irlanda*,[15] por ejemplo, el Tribunal Europeo de Derechos Humanos (TEDH) sostuvo que la decisión del Gobierno irlandés de incautar un

avión en Dublín que pertenecía a una empresa turca fue suficiente para interponer, dentro de la jurisdicción de la República de Irlanda, una demanda contra la empresa turca para los efectos del procedimiento.

El mismo principio se ha aplicado también en los casos de vigilancia. En el caso de 2008 de *Liberty y otros v. Reino Unidos*,[16] dos ONG irlandesas habían protestado contra el de sus comunicaciones privadas por el gobierno británico a través de su Fondo de Prueba Electrónica en Capenhurst en Cheshire, Inglaterra, una instalación capaz de controlar 10.000 conversaciones simultánea entre Irlanda y Europa. En ese caso, la Gran Sala del TEDH encontró una violación al derecho a la intimidad de las ONGs irlandesa en virtud del artículo 8 del Convención Europea de Derechos Humanos (CEDH) a pesar de que ninguna de las organizaciones no gubernamentales se encontraba físicamente presente en el territorio del Reino Unido. En una anterior decisión de admisibilidad en *Weber & Savaria v. Alemania*,[17] el TEDH se pronunció de forma similar al considerar las quejas de dos residentes de Uruguay contra el monitoreo de sus telecomunicaciones por parte del gobierno alemán.[18]

La tendencia generalizada en cada uno de estos casos es que la vigilancia se estaba llevando a cabo *en* el territorio del Estado en cuestión, aunque los sujetos de la vigilancia no lo estaban. La obligación contraída por el Estado bajo el derecho internacional de los derechos humanos de respetar los derechos de todas las personas dentro de su territorio o jurisdicción, por tanto, *incluye* a las personas físicamente fuera del Estado, pero cuyos derechos están siendo interferidos por las acciones que un Estado realiza dentro de sus fronteras.

También es importante tener en cuenta que la jurisdicción territorial puede surgir no solo sobre la base de la ubicación física en donde ocurre la vigilancia de las comunicaciones privadas, sino también en donde se *procesan* los datos. En otras palabras, incluso si el gobierno británico hubiese capturado las llamadas

telefónicas privadas de las ONG irlandesas desde, por ejemplo, una instalación situada fuera del Reino Unido, su jurisdicción territorial aún estaría comprometida si los datos de las llamadas telefónicas hubiesen sido procesados por los organismos gubernamentales *dentro* del Reino Unido.

Incluso cuando la vigilancia por parte del Estado ocurre fuera de su territorio, éste seguiría siendo responsable de violaciones a los derechos humanos en aquellos lugares en los que tendría autoridad o control efectivo. Así lo estableció el Comité de Derechos Humanos de las Naciones Unidas en *López Burgos v. Uruguay* y *Celiberti de Casariego v. Uruguay*:[19]

> Los Estados Partes están obligados por el artículo 2, párrafo 1, a respetar y garantizar los derechos reconocidos en el Pacto a todos los individuos que se encuentren en su territorio y a todas las personas sometidas a su jurisdicción. Esto significa que un Estado Parte debe respetar y garantizar los derechos establecidos en el Pacto a cualquier persona sometida al poder o al control efectivo de ese Estado Parte, aunque no se encuentre en el territorio del Estado Parte.

El Tribunal Europeo de Derechos Humanos también ha sostenido que:[20]

> ...En circunstancias excepcionales, los actos de los Estados contratantes que se hayan realizado en su territorio o que produzcan efectos allí ("acto extraterritorial") podría equivaler al ejercicio de su jurisdicción en el sentido del artículo 1 de la Convención.

Algunos gobiernos, sobre todo los de EE.UU. e Israel, han negado que sus obligaciones bajo el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) se extiendan a los actos realizados fuera de su territorio.[21] En el contexto de los debates sobre el Proyecto de Resolución de la Asamblea General de las Naciones Unidas sobre *El derecho a la privacidad en la era di-*

gital—presentada en respuesta a las revelaciones de Snowden—se filtró una nota informativa en donde se confirma que EE.UU. sigue defendiendo la posición de que no tiene ninguna deber legal de cumplir con el artículo 17 del PIDCP (intimidad) fuera de su territorio geográfico. De hecho, consideraba que era una delimitación o "línea roja" que no iba a cruzar. Su primera instrucción fue que los negociadores estadounidenses debería:[22]

> Aclarar que las referencias al derecho a la intimidad se refiere de manera explícita a las obligaciones de los Estados bajo el PIDCP y *retirar la sugerencia de que tales obligaciones son de aplicación extraterritorial*. [Énfasis añadido]

La posición de Estados Unidos con respecto a la inaplicabilidad del Pacto sobre sus actividades extraterritoriales fue duramente criticada por el Comité de Derechos Humanos de las Naciones Unidas en su 110º período de sesiones.[23] Como señaló el Comité:

> ¿Podría la delegación reconocer que la posición de Estados Unidos sobre las actividades extraterritoriales ha permitido a Estados Unidos cometer infracciones en todas partes menos en su propio territorio? La no aplicabilidad del Pacto a las actividades extraterritoriales ha dado lugar a la impunidad y a violaciones de los derechos. Si todo los Estados compartiesen esta interpretación, no habría ninguna protección de derechos.

Como se desprende de lo antes expuesto, este rancio punto de vista de EE.UU. sobre sus obligaciones bajo el PIDCP claramente está en contradicción con el derecho internacional de los derechos humanos.[24] Esto fue reconocido por la Asamblea General de las Naciones Unidas, que finalmente rechazó las sugeridas delimitaciones estadounidenses y explícitamente reconoció en un considerando que la vigilancia extraterritorial plantea preocupaciones en torno a los derechos humanos:

> Profundamente preocupada por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales, en particular cuando se llevan a cabo a gran escala[25]

Ya sea como un asunto de jurisdicción extraterritorial o por medio de una aplicación directa de los principios de jurisdicción territorial, está claro que los Estados no pueden eludir su obligación de respetar la privacidad de las comunicaciones en relación con la nacionalidad de los participantes o su localización física. Por esta razón, los Principios hacen explícita la necesidad de los Estados de actuar de forma no discriminatoria, independientemente de factores como raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

Definiciones:

"INFORMACIÓN PROTEGIDA" Y "VIGILANCIA DE LAS COMUNICACIONES"

Los Principios abordan dos cuestiones centrales de definición que han planteado problemas específicos en la aplicación de la protección de los derechos humanos a las técnicas avanzadas de vigilancia de las comunicaciones. La primera se refiere a qué tipo de información está protegida. En cuanto a las prácticas de vigilancia del Estado, ha habido una tendencia a creer que ciertos tipos de datos son menos dignos de protección, basado en analogías artificiales que son anteriores a la llegada de las redes digitales, a pesar de la naturaleza altamente reveladora y sensible de los datos. Los Principios atienden esto al definir "información protegida" que incluyen estas categorías de información y reconocen las consecuencias de su intervención en los

derechos humanos. En segundo lugar, los avances tecnológicos han permitido a las entidades estatales controlar, analizar, recopilar y almacenar cantidades masivas de información de manera indefinida. Dado que estas actividades pueden llevarse a cabo sin que una persona "busque" de forma directa una información específica, hay quienes argumentan que los intereses privados no están involucrados o no están limitados. Sin embargo, estas actividades de vigilancia impactan dramáticamente la intimidad de las personas y, en efecto, producen cantidades significativas de información disponible, que de lo contrario no estarían al alcance. Por otra parte, el fundamento jurídico de estas distinciones es dudoso. Los Principios definen de manera amplia la "vigilancia de las comunicaciones" para abarcar un considerable espectro de actividades que afectan los valores de la intimidad y la expresión inherentes a las redes de comunicaciones.

INFORMACIÓN PROTEGIDA

En pocos años, las tecnologías de las comunicaciones han experimentado cambios sin precedentes, como también el uso intensivo de esas tecnologías por personas en todo el mundo. Al mismo tiempo, gran parte de la legislación vigente y la jurisprudencia que trata sobre las salvaguardias contra la vigilancia intrusiva fueron desarrollados hace varias décadas—en los días en que las llamadas telefónicas eran operadas por la marcación de tonos y los computadores personales eran una rareza.

En lugar de mantener conceptos obsoletos y categorías de una época pre-digital, los Principios han sido redactado de forma tal que reflejan la forma en la que hoy día se almacenan y comparten los datos tanto por organismos públicos como privados, y para proporcionar un nivel de protección que corresponda a la realidad de los daños resultantes cuando el Estado accede incorrectamente a los datos.

En concreto, los Principios utilizan el término "información protegida" para referirse a la información (incluyendo los datos) que debe ser plena y sólidamente protegida, aun cuando la información no esté protegida por la ley, esté parcialmente protegida por la legislación, o se conceda niveles más bajos de protección. La intención, sin embargo, no es establecer una nueva categoría que con el tiempo se haga arcaica, sino más bien asegurar que el foco es y seguirá siendo la capacidad de la información, sola o combinada con otra información, para revelar hechos privados acerca de un persona o sus corresponsales. Como tal, los Principios adoptan una definición única y global que incluye cualquier información relacionada con las comunicaciones de una persona que no son de fácil acceso al público en general.

Aunque recientemente los tribunales han comenzado a resistir este enfoque, algunas legislaciones de América del Norte, Europa, Asia y América Latina han hecho una distinción de larga data entre el "contenido" de un mensaje (el mensaje real), los "datos de las comunicaciones" o "metadatos" (como sería la información acerca de quién envió un mensaje a quién y cuándo o dónde se envió el mensaje),[26] y los "datos del suscriptor" (datos sobre el propietario de una cuenta involucrada en una comunicación).[27] Siguiendo esta distinción, tradicionalmente, algunas leyes de Norteamérica, Europa, Asia y América Latina han otorgado mayor protección contra intervenciones al *contenido* de las comunicaciones de una persona que a los datos relativos a dicha comunicación. Como es de esperar, esta diferenciación se basa en el modelo tradicional del servicio postal, que distingue entre la información escrita en el sobre y el contenido del sobre (de hecho, los "datos del sobre" frecuentemente se usa como un sinónimo de los "datos de las comunicaciones" o los "metadatos"). Esta antigua distinción, sin embargo, carece de sentido debido a los modernos métodos de interceptación; a diferencia del correo postal convencional; por ejemplo, la interceptación del correo electrónico consiste en que el contenido y los metadatos estén disponibles de manera inmediata a los organismos que se

encargan de realizar dicha intervención. Por otra parte, hoy en día los proveedores de servicio almacenan los metadatos en formatos digitales y pueden adquirirlos masivamente a través de órdenes de producción en formas que no tienen equivalente en el servicio postal.[28] Además, no hay comparación "postal" con la gran cantidad de actividad anónima en línea que se puede vincular a una persona cuando la información del suscriptor es revelada al Estado.[29]

Estas distinciones fueron adoptadas como una especie de medida aproximada a la intimidad—la idea de que simplemente conociendo quien recibió la carta en un determinado momento no fuese tan reveladora como el contenido mismo de la carta. Sin embargo, el aumento en la abundancia de metadatos, y las técnicas de acumulación y análisis de la misma, significa que incluso "simples metadatos" son capaces de revelar mucho más acerca de las actividades o pensamientos de un individuo que lo que sucedía hace treinta o cuarenta años atrás. Esto se debe, en parte, a la creciente cantidad y al alcance de los datos recolectados: A principios de 1980, por ejemplo, cuando el Tribunal Europeo de Derechos Humanos atendió por primera vez una denuncia sobre el uso de medidores telefónicos[30] para recopilar detalles de las llamadas telefónicas de un sospechoso, la única información que se registraba eran los números de teléfono llamados y la duración de las llamadas telefónicas. En la actualidad, los organismos estatales buscan recopilar no solo las identidades de las personas que llaman, sino también sus datos de facturación, direcciones, datos de tarjetas de crédito, marca y modelo de los teléfonos usados, y datos de localización geográfica de sus movimientos físicos. En el caso de la navegación por Internet, un simple URL escrito en un navegador de Internet (que en algunas jurisdicciones se considera "metadato", mas no contenido),[31] puede ser tan reveladora—y en ocasiones aún más reveladora—que el contenido real de un sitio web.[32] Del mismo modo, en un ecosistema donde los individuos dejan sus huellas electrónicas tras todas sus interacciones digitales, la identificación del propietario

de la dirección IP, el identificador de un dispositivo móvil o la dirección IP de un correo electrónico, un identificador del abonado móvil (IMSE) o una dirección de correo electrónico pueden ser tremendamente reveladores. De este modo, los metadatos pueden ser un "*proxy* de contenido".[33] Además, hoy día la gente simplemente usa las tecnologías de las comunicaciones con más frecuencia que cuando las comunicaciones se hacían, mayormente, a través de cartas. Por último, e igualmente importante, la capacidad del gobierno para recopilar mucho más de estos datos, por un largo periodo de tiempo y organizándolos por medio de modernas técnicas de vigilancia permiten crear un retrato íntimo de la vida de una persona a partir de simples metadatos.

La relativa falta de protección de los metadatos de una persona se hace particularmente evidente bajo el derecho constitucional de los EE.UU.—aunque es cada vez más común encontrar tribunales estadounidenses y de otros países que reconocen la imposibilidad de aplicar esta distinción a las comunicaciones modernas. Aunque la Cuarta Enmienda protege el *contenido* de las comunicaciones de una persona con terceros,[34] y si bien no hay ningún tribunal que haya tomado una decisión definitiva con respecto al tipo de vigilancia masiva llevada a cabo por la NSA tras el 11S, los tribunales estadounidenses han sostenido que la aplicación de la Cuarta Enmienda no se aplica a la información que una persona comparte "voluntariamente" con terceros (la llamada "doctrina del tercero"), incluyendo los detalles de sus registros telefónicos en poder de la compañía telefónica:[35]

> Los usuarios de teléfonos...normalmente saben que deben transmitir información numérica a la compañía telefónica; que la compañía telefónica cuenta con instalaciones para la grabación de esta información; y que la compañía telefónica, de hecho, registra esta información para una variedad de fines comerciales legítimos. Aunque las expectativas subjetivas no se

> pueden medir científicamente, es exagerado creer que los suscriptores del servicio telefónico, en estas circunstancias, albergan alguna expectativa general de que los números marcados permanecerán en secreto.

Con los avances tecnológicos de las comunicaciones, la conclusión de los tribunales de Estados Unidos de que no hay ninguna expectativa de intimidad en los registros telefónicos se ha extendido a otras formas de comunicación. Por ejemplo, en el caso de 2008 de *Estados Unidos v. Forrester*, 512 F. 3d 500, la Corte del Noveno Circuito de Apelaciones sostuvo que:

> Los correo electrónico y los usuarios de Internet no tienen ninguna expectativa de intimidad en las direcciones de sus mensajes enviados o recibidos y las direcciones IP de los sitios web que visitan, pues, deben saber que esta información es proporcionada y utilizada por los proveedores de servicios de Internet con el fin de dirigir el enrutamiento de la información.

Sin embargo, en el reciente caso de la Corte Suprema *Estados Unidos v. Jones*, 132 S. Ct. 949 (2012), la jueza Sotomayor pareció estar dispuesta a considerar un cambio en este enfoque. Según sus propias palabras, en referencias a otros casos, señaló que:

> No asumiría que toda la información voluntariamente revelada a algún miembro del público para un propósito limitado carecería por esa sola razón de la protección de la Cuarta Enmienda. Véase *Smith*, 442 EE.UU. en 749 ("La intimidad no es un producto discreto, que importa total o absolutamente. Quienes revelan ciertos hechos a un banco o a una compañía de teléfono para un propósito comercial limitado no están obligados a asumir que esta información se dará a conocer a otras personas para otros fines"); *véase también Katz*, 389 U.S. 351-352 ("[L]o que [una persona] busca preservar como privado,

incluso en una área disponible al público, puede estar protegida por la Constitución.").

El caso *Jones* se decidió por otros motivos, por lo que este punto de vista no ha sido adoptado aún por la Corte Suprema. No obstante, recientemente el Grupo de Revisión del Presidente de los Estados Unidos en su informe sobre Inteligencia y Tecnologías de las Comunicaciones cuestionó este planteamiento.[36]

Como los tribunales estadounidenses aún no han reconocido garantías constitucionales a los metadatos, actualmente, éstos están protegidos sobre todo a través de regímenes legislativos, como el *Pen Register Statute*,[37] que otorga menos protección a estos datos que al "contenido". Esto, a su vez, ha inspirado leyes similares en otros países como en Corea, en donde la adquisición de los metadatos está condicionada a la autorización del tribunal.[38]

Por el contrario, el Tribunal Europeo de Derechos Humanos ha reconocido a los datos de las comunicaciones como "un elemento integral" de una comunicación privada y por lo tanto goza de cierto grado de protección bajo el derecho a la intimidad reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH), aunque menos que la otorgada al contenido de una comunicación.[39] Otros tipos de datos personal (incluidos los datos que no son comunicaciones) también gozan de protección bajo la ley de protección de datos de Europa[40] y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que dispone que toda persona tiene derecho a la protección de sus datos personales, lo que, en principio, debería extenderse a los metadatos y a la información del suscriptor. Resulta alentador que la Gran Sala del Tribunal de Justicia de la Unión Europea rechazara hace poco el argumento de que los "metadatos" deben tener una protección menor que el "contenido" de las comunicaciones en el contexto del artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea.[41] Al mismo tiempo, está claro

que la legislación europea en este ámbito también sufre de serios problemas: en primer lugar, como se ha señalado anteriormente, la distinción de larga data entre los metadatos o los datos de las comunicaciones, por un lado, y el contenido de las comunicaciones, por el otro, se ve erosionada por los cambios tecnológicos; en segundo lugar, no está claro en qué medida la protección otorgada a los datos de las comunicaciones bajo el artículo 8 del CEDH, y que protege a otros tipos de datos personal bajo la legislación de protección de datos, se superponen entre sí. Esto es particularmente problemático dado que la legislación europea de los derechos humanos y la ley de protección de datos de la Unión Europea son cada una capaz de proteger la misma información de maneras muy diferentes, y están sujetas a diferentes excepciones.[42]

A la luz de estos problemas, está claro que ya no es sensata la distinción existentes entre los metadatos y el contenido, y que es necesario un nuevo enfoque para proteger la intimidad individual en la era digital. Por tanto, los Principios se cimentan sobre la base de que toda la información relativa a las comunicaciones privadas de una persona debería ser considerada como "información protegida", y, en consecuencia, debería obtener la más sólida protección legal. En la medida en que es necesario proporcionar mayores niveles de protección según el caso, esto debería depender de la naturaleza de la intrusión en un contexto particular, y no en referencia a categorías abstractas y definiciones arcaicas.

VIGILANCIA DE LAS COMUNICACIONES

A raíz de las revelaciones de Snowden, varios gobiernos han procurado de manera más agresiva defender sus actividades mediante la distinción entre la recogida automatizada y el escaneo de las comunicaciones privadas, por un lado, y el escrutinio real de dichas comunicaciones por seres humanos, por el otro. Algunos funcionarios han sugerido que si la información es simplemente recopila y almacenada pero no es analizada

por un humano, entonces, no se produce ninguna invasión a la intimidad. Otros argumentan que los computadores que analizan todas las comunicaciones en tiempo real a través de palabras clave y otros selectores, no puede considerarse "vigilancia" para los efectos de la activación de las protecciones legales.

El derecho internacional de los derechos humanos, sin embargo, deja claro que la recopilación y retención de datos de las comunicaciones equivale a una injerencia en el derecho a la intimidad, con independencia de que los datos sean posteriormente puestos a disposición o utilizados por funcionarios del gobierno. En *S & Marper v. Reino Unido*, por ejemplo, la Gran Sala del Tribunal Europeo de Derechos Humanos sostuvo que "la mera retención y almacenamiento de datos personales por parte de las autoridades públicas, sin importar cómo se obtuvieron, debe considerarse como que tiene un impacto directo en el interés de la vida privada de la persona afectada, con independencia de los usos posteriores que se hagan de los datos".[43] En *Digital Rights Ireland Ltd v.l Ministro para las Comunicaciones*, la Gran Sala del Tribunal de Justicia de la Unión Europea igualmente señaló que la retención de los datos de las comunicaciones "a los efectos de un posible acceso a ellos por las autoridades nacionales competentes" constituía una "interferencia particularmente grave" con el derecho al respeto de la vida privada y familiar, del domicilio y de las comunicaciones bajo el artículo 7 de la Carta de los Derechos fundamentales de la UE.[44]

Por estas razones, los Principios establecen manifiestamente que la "Vigilancia de las Comunicaciones" incluye la lectura real de las comunicaciones privadas por otro ser humano, como también toda la gama de monitoreo, interceptación, recopilación, análisis, uso, conservación y retención de, la interferencia con, o el acceso a la información que incluye, refleja, o surge de las comunicaciones pasadas, presente o futuras de una persona. Cualquier sugerencia de los gobiernos de que la captación o monitoreo no es vigilancia es, por lo tanto, contraria a las exigencias del derecho internacional de los derechos hu-

manos. Tampoco los Estados deben saltarse las protecciones de privacidad en función de estas definiciones arbitrarias.

EXPLICACIÓN PRINCIPIO POR PRINCIPIO

Los Principios están firmemente enraizados en el derecho internacional de los de derechos humanos. En concreto, se fundamentan en los derechos a la intimidad, a la libertad de opinión y de expresión, y a la libertad de asociación, garantizados en la Declaración Universal de los Derechos Humanos (DUDH), el Pacto Internacional de Derechos Civiles y Políticos (PIDCP), la Convención Europea de Derechos Humanos (CEDH), la Carta Europea de Derechos Fundamentales (Carta de la UE) y la Convención Interamericana de Derechos Humanos (CIDH).[45]

Aunque cada uno de estos derechos se formula en formas ligeramente diferentes,[46] la estructura de cada artículo se divide en dos partes. En el primer párrafo se establece el contenido básico del derecho, mientras que en el segundo párrafo se señalan las circunstancias en las que ese derecho puede ser restringido o limitado. Típicamente, el segundo párrafo dispone que cualquier restricción al derecho fundamental debe cumplir con los siguientes requisitos:

- Debe estar provista por la ley;
- No debe ser "arbitraria";
- Debe tener uno de los objetivos legítimos enumerados taxativamente en ese párrafo; y
- Debe ser necesario para alcanzar los objetivos en cuestión—que se ha decidido que incluyan requisitos de idoneidad y proporcionalidad.

Este examen de "limitaciones permisibles" se ha aplicado por igual a los derechos a la intimidad, a la libertad de expresión y a la libertad de asociación.[47] Más adelante exponemos con más

detalle el fundamento legal de cada uno de estos requisitos en el título correspondiente a cada Principio (Principios 1 al 5). En su caso, lo hacemos teniendo en cuenta el contexto específico de la vigilancia. Acto seguido, planteamos nuestro pensamiento y fundamento jurídico detrás de la adopción de los restantes Principios (Principios 6 al 13). Aunque los abordamos por separado, hacemos hincapié en que los Principios son integrales y autoreferenciales, lo que significa que cada principio y el preámbulo deberían ser leídos e interpretados como parte de un marco más amplio.

PRINCIPIO 1: LEGALIDAD

Principio general

El principio de legalidad es un elemento fundamental de todos los instrumentos internacionales de derechos humanos y, de hecho, del Estado de Derecho en general. Es una garantía básica contra el ejercicio arbitrario de las facultades del Estado. Por esta razón, cualquier restricción a los derechos humanos debe estar "prevista" o "proscrita" por la ley.[48]

En el PIDCP el principio de legalidad está estrechamente relacionado con el concepto de "injerencias arbitrarias". Por ejemplo, el artículo 17 dispone que *"[n]adie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, o su correspondencia*". El Comité de Derechos Humanos ha interpretado "injerencias arbitrarias" de la siguiente manera:[49]

> La expresión "injerencias arbitrarias" atañe también a la protección del derecho previsto en el Artículo 17. A juicio del Comité, la expresión "injerencias arbitrarias" puede extenderse también a las injerencias previstas en la ley. Con la introducción del concepto de arbitrariedad se pretende garantizar que incluso cualquier injerencia prevista en la ley esté en consonancia con las disposiciones, los propósitos y los objetivos del Pacto y sea, en todo caso, razonable en las circunstancias particulares.

El significado de "ley" también implica ciertos requisitos mínimos cualitativos de claridad, accesibilidad y previsibilidad. En particular, el Comité de Derechos Humanos ha explicado en detalle qué se entiende por "ley" a los efectos del artículo 19 del PIDCP (libertad de opinión y de expresión) en los términos siguiente:[50]

> 25. A los efectos del párrafo 3, una norma, que se caracteriza como una "ley", debe ser formulada con la suficiente precisión para permitir que una persona regule su conducta en consecuencia y debe ser accesible al público. Una ley no puede conferir una facultad discrecional para la restricción de la libertad de expresión a los encargados de su ejecución. Las leyes deben proporcionar suficiente orientación a los encargados de su aplicación a fin de que puedan determinar qué tipo de expresiones están debidamente restringidas y qué tipos no lo están.

El Tribunal Europeo de Derechos Humanos ha seguido un planteamiento similar en su jurisprudencia. En concreto, ha sostenido que la expresión "prevista por la ley" implica los siguientes requisitos:[51]

> En primer lugar, la ley debe ser suficientemente accesibles: el ciudadano debe ser capaz de tener una indicación de qué es adecuado en las circunstancias de las normas legales aplicables a un caso concreto. En segundo lugar, una norma no puede ser considerada como una "ley" a menos que esté formulada con la suficiente precisión para permitir al ciudadano regular su conducta; debe ser capaz—si es preciso con un asesoramiento adecuado—de prever, en un grado que sea razonable a las circunstancias, las consecuencias de un determinado acto.

Los mismos requisitos se aplican en relación con el derecho a la intimidad bajo el artículo 17 del PIDCP y el artículo 8 del

CEDH.[52] En concreto, el Tribunal Europeo de Derechos Humanos ha aclarado en el contexto de la vigilancia que:[53]

> [L]a ley debe ser suficientemente clara en sus términos para dar a los ciudadanos una indicación adecuada sobre las circunstancias y las condiciones en las que los poderes públicos están facultados a recurrir a esta interferencia secreta y potencialmente peligrosas con el derecho al respeto de la vida privada y la correspondencia.

El Tribunal Europeo continuó explicando que:[54]

> [S]ería contrario al Estado de la Derecho que se expresara la discrecionalidad legal concedida al ejecutivo en términos de un poder ilimitado. En consecuencia, la ley debe indicar el alcance de dicho poder discrecional conferido a las autoridades competentes y la forma de su ejercicio con suficiente claridad, teniendo en cuenta el objetivo legítimo de la medida en cuestión, para dar al individuo una protección adecuada contra interferencias arbitrarias.

En otras palabras, las normas o directrices secretas o las interpretaciones normativas no tienen calidad de "ley".[55] Una legislación que no es pública no es una ley, ya que es un componente esencial del Estado de Derecho que las leyes sean conocidas y accesible a todos. Del mismo modo, las leyes o regulaciones que se expresan en términos de un poder ilimitado otorgado a las autoridades entran en conflicto con los requisitos de la "ley". Por tanto, el alcance y la forma de ejercicio de cualquier discreción deben indicarse en la propia ley o en las directrices publicadas con "razonable claridad", para que los individuos pueden razonablemente prever cómo se aplicará la ley en la práctica. Esto es aún más importante dado los riesgos inherentes de la arbitrariedad en el ejercicio del poder en secreto.[56]

En el contexto de la vigilancia, esto significa que la adopción de una ley que autoriza la vigilancia masiva a nivel nacional no hace lícita la vigilancia, si de entrada esa ley no cumple con ciertos requisitos básicos de claridad y accesibilidad.

Salvaguardas mínimas en el contexto de la vigilancia de las comunicaciones

Los antes mencionados requisitos de claridad, accesibilidad y precisión adquieren un significado especial en el contexto de la vigilancia de las comunicaciones. Esto se debe a la distintiva amenaza que presenta la vigilancia secreta a la esencia misma de la democracia, como reconoció el Tribunal Europeo de Derechos Humanos en 1978.[57] El Tribunal consideró que la "mera existencia" de una legislación que permitía un sistema de monitoreo secreto de las comunicaciones dio lugar a una "amenaza de vigilancia", que equivalía a una interferencia con la privacidad de *todos* aquellos a los que la legislación haya sido aplicada.[58] En vista de estos riesgos, el Tribunal llegó a la conclusión de que deben existir garantías adecuadas y suficientes contra los abusos establecidos en la ley, y más concretamente en los decretos.[59]

En particular, el Tribunal Europeo de Derechos Humanos ha identificado las siguientes garantías mínimas que una ley de vigilancia debe reunir para que sea compatible con el artículo 8 del CEDH:[60]

- Deben precisarse de manera clara y concreta los delitos y actividades que se ordena con la vigilancia
- La ley debe indicar manifiestamente qué categorías de personas pueden ser sometidas a la vigilancia;
- Deben fijarse plazos estrictos para las operaciones de la vigilancia;

- Deben establecerse procedimientos estrictos para ordenar el análisis, uso y almacenamiento de los datos obtenidos a través de la vigilancia;
- La ley debe establecer las precauciones que deben tomarse cuando se comunican datos a terceros;
- Deben fijarse normas estrictas sobre la destrucción o supresión de los datos de vigilancia para prevenir que la vigilancia se mantenga oculta tras los hechos;
- Los organismos encargados de supervisar el uso de las facultades de vigilancia deben ser independientes y responsables, y serán nombrados por el Parlamento y no por el Poder Ejecutivo.

El mismo criterio se ha seguido en las Naciones Unidas y a nivel interamericano. En concreto, los Relatores Especiales de las Naciones Unidas y la OEA para la libertad de expresión recientemente emitieron una declaración conjunta sobre los programas de vigilancia en el que indicaban:[61]

> [L]os Estados deben garantizar que la interceptación, recolección y uso de información personal, incluidas todas las limitaciones al derecho de la persona afectada a acceder a esta información, estén claramente autorizada por la ley a fin de proteger a las personas contra injerencias arbitrarias o abusivas en su 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.
>
> Dada la importancia del ejercicio de estos derechos para el sistema democrático, la ley debe autorizar el acceso a las comunicaciones y a datos personales solo en las circunstancias más excepcionales definidas en la legislación. Cuando se invoque la seguridad nacional como

> razón para vigilar la correspondencia y los datos personales, la ley debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resulta legítimo. Su aplicación deberá autorizarse únicamente cuando exista un riesgo cierto respecto de los intereses protegidos, y cuando ese daño sea superior al interés general de la sociedad en función de mantener el derecho a la privacidad [sic] y a la libre expresión del pensamiento y circulación de información. La entrega de esta información debe ser monitoreada por un organismo de control independiente y contar con garantías suficientes de debido proceso y supervisión judicial, dentro de las limitaciones permisibles en una sociedad democrática.

Sus puntos de vista reflejan también las recomendaciones del Relator Especial de las Naciones Unidas para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, Martin Scheinin, que afirmó en su informe de 2009:[62]

> 62. Se deben establecer mandatos de supervisión estrictos e independientes para examinar las políticas y prácticas a fin de garantizar la existencia de una rigurosa supervisión del uso de técnicas intrusivas de vigilancia y del procesamiento de la información personal. Por consiguiente no debe haber ningún sistema secreto de vigilancia que no se encuentre sometido al examen de un órgano de supervisión efectivo y todas las injerencias deben ser autorizadas por un órgano independiente.

Más adelante, respecto a las Principios 6, 7, 9 y 10, retomamos la obligación de contar con una fuerte supervisión independiente.

PRINCIPIO 2: OBJETIVO LEGÍTIMO

Bajo el derecho internacional de los derechos humanos, cualquier restricción a los derechos a la intimidad, a la libertad de

expresión y a la libertad de asociación debe perseguir al menos uno de los "objetivos legítimos", que a menudo se enumeran taxativamente en el artículo correspondiente. Estos objetivos han sido formulados de manera muy amplia e incluyen seguridad pública, prevención del delito, protección de la moralidad y de los derechos de los demás, y seguridad nacional.[63] El artículo 8 del CEDH también incluye "el bienestar económico del país". Si bien el artículo 17 del PIDCP explícitamente no dispone que ninguna restricción al derecho a la intimidad deba ser necesaria para un propósito determinado, tanto el Relator Especial de las Naciones Unidas para la Lucha contra Terrorismo como el Relator Especial de las Naciones Unidas para la Libertad de Expresión ha sostenido que el examen de "limitaciones permisibles" bajo el Artículo 19, entre otros artículos del Pacto, es igualmente aplicable al artículo 17 del PIDCP.[64]

En el derecho europeo de los derechos humanos, los Estados rara vez se encuentran con alguna dificultad en demostrar que la restricción controvertida persigue un objetivo legítimo. Esto se debe a que el Tribunal tiende a enfocar su análisis en el marco legal para el ejercicio de las facultades de vigilancia y no en una medida de vigilancia usada en un caso particular. Además, el Tribunal generalmente ha aceptado que las facultades de vigilancia son necesarias para los fines de la seguridad nacional y del orden público.[65] La necesidad de que las medidas de vigilancia estén más específicamente "dirigidas" es un aspecto que tiene más que ver con la cuestión de proporcionalidad de la medida, pero, en la práctica, el Tribunal rara vez lo ha examinado.[66]

Por el contrario, el Relator Especial de la Naciones Unidas para la Libertad de Expresión, Frank La Rue, en un reciente informe, expresó su preocupación indicando que las "vagas y no especificadas" nociones de "seguridad nacional" se han utilizado indebidamente para justificar la interceptación y el acceso a las comunicaciones sin garantías adecuadas.[67] El Relator Especial llegó a la conclusión de que:

> 60. Es motivo de grave preocupación el uso de un concepto amorfo de seguridad nacional a fin de justificar limitaciones invasivas al disfrute de los derechos humanos. El concepto se define en términos amplios y por lo tanto está más expuesto a la manipulación por parte del Estado como un medio para justificar acciones dirigidas a grupos vulnerables, como los defensores de derechos humanos, periodistas o activistas. También actúa para permitir el secreto a menudo innecesario en torno a las investigaciones de los encargados de aplicar la ley, socavando los principios de transparencia y rendición de cuentas.[68]

Consciente del potencial abuso inherente a conceptos demasiado amplios, los Principios han tratado de adoptar una norma más estricta sobre lo que constituye un "objetivo legítimo" respecto a la vigilancia masiva. Por esta razón, también se descartaron el examen de "objetivos apremiantes y sustanciales" aplicado en Canadá y el examen del "interés gubernamental apremiante" que se utiliza en los Estados Unidos por no ser suficientemente rigurosos.[69] En cambio, los Principios reflejan el estándar más alto impuesto en Alemania. El Tribunal Constitucional alemán ha dictaminado que las medidas profundamente invasivas tales como el registro de un computador por los organismos del orden público no puede justificarse únicamente teniendo en cuenta algún interés general vagamente definido. Este Tribunal consideró que una medida de este tipo tenía que estar justificada a la luz de pruebas que demuestren "una amenaza concreta a un importante interés protegido jurídicamente", como una amenaza a "la vida, integridad física o libertad de una persona" o a "bienes públicos, a los cimientos o existencia del propio Estados, o de las condiciones básicas de la existencia humana".[70]

Además, los Principios prohíben expresamente la discriminación en las leyes, incluida la discriminación basada en el origen nacional o social, nacimiento o cualquier otra condición

social. Esto es, por supuesto, una disposición estándar del derecho internacional de los derechos humanos.[71] Aquí, junto con la aplicación extraterritorial de la ley que ya se discutió antes, nos aseguramos que las protecciones legales alcancen a todas las personas sujetas a vigilancia, independientemente de su ubicación o nacionalidad.

PRINCIPIOS 3, 4, 5: NECESIDAD, IDONEIDAD & PROPORCIONALIDAD

Es una de las piedras angulares de las normas de derechos humanos el principio de que cualquier injerencia en un derecho calificado, como el derecho a la intimida o a la libertad de expresión, sea "necesario en una sociedad democrática". En general, esto significa que un Estado no solo debe demostrar que su injerencia en el derecho de una persona satisface una "necesidad social imperiosa", sino también que es *proporcional*—o en la jurisprudencia interamericana, *adecuada*[72]—al objetivo legítimo perseguido.[73]

En particular, el Tribunal Europeo de Derechos Humanos ha aclarado que el término "necesario" no es sinónimo de "indispensables". Tampoco es tan flexible como los términos "admisible", "ordinario", "útil", "razonable" o "deseable".[74] Sujeto a la doctrina del "margen de apreciación", el Tribunal Europeo hace su evaluación de la necesidad y proporcionalidad de una medida "a la luz de todas las circunstancias". Sin embargo, ciertas medidas, como la facultad de vigilancia secreta, son analizadas desde un enfoque más estricto.[75]

El Comité de Derechos Humanos ha seguido un planteamiento similar. En concreto, la Comisión explicó en su Observación General sobre el artículo 12 del PIDCP (libertad de movimiento) que:[76]

> El párrafo 3 del artículo 12 indica claramente que no basta con que las restricciones se utilicen para conseguir

> fines permisibles; también deben ser necesarias para protegerlos. Las medidas restrictivas deben ajustarse al principio de proporcionalidad; deben ser adecuadas para desempeñar su función protectora; *deben ser el instrumento menos perturbador de los que permitan conseguir el resultado deseado*, y deben guardar proporción con el interés que debe protegerse. [Énfasis añadido].

Los mismos principios se aplican a la interpretación de los artículos 19[77] y 17[78] del PIDCP.

El Comité de Derechos Humanos en ocasiones ha usado la palabra "apropiada" en su análisis. Por ejemplo, en relación con el artículo 19 del PIDCP (libertad de expresión), el Comité observó que las medidas restrictivas "deben ser apropiadas para desempeñar su función protectora".[79]

Igualmente, como se señaló antes, la Corte Interamericana de Derechos Humanos algunas veces se ha referido al concepto de "idoneidad". En concreto, la Corte ha considerado si las medidas en cuestión serían capaces de contribuir a la realización de los objetivos invocados para limitar el derecho en cuestión.[80]

Los tribunales de varios estados han aclarado que sustantivamente la "idoneidad" o "apropiado" no quiere decir que las medidas en cuestión tengan que ser especialmente satisfactorias. En su lugar, imponen un requisito análogo al concepto canadiense de "racionalmente vinculado", aunque la "idoneidad" se aplica con más rigor. La medida no solo debe tener alguna relación lógica con el objetivo previsto, sino también debe ser "eficaz" en lograrlo. Una medida que es inherentemente incapaz de alcanzar el objetivo establecido, o que es manifiestamente ineficaz en el alcanzarlo, no puede decirse que es "idónea", "necesaria" o "proporcional".

Este requisito de proporcionalidad es particularmente importante en el contexto de la vigilancia masiva, que se basa en la

captación indiscriminada y la retención de las comunicaciones y metadatos sin estar dirigidas o tener sospecha razonable. En *S y Marper*, por ejemplo, la Gran Sala del Tribunal Europeo de Derechos Humanos sostuvo que la retención "ilimitada e indiscriminada" de datos del ADN equivale a una "injerencia desproporcionada" en la vida privada de aquellas personas a quien pertenecían los datos tomados. La Gran Sala hace especial hincapié en el hecho de que el material fue "retenido indefinidamente, cualesquiera haya sido la naturaleza o gravedad del delito presuntamente cometido por la persona".[81] En otro caso relacionado con el uso de las facultades de registro, la Gran Sala encontró que la ausencia de una requisito sobre la "sospecha razonable" de la policía de que la persona buscada había participado en una actividad criminal significaba que la facultad de registro carecía de "garantías legales adecuadas contra abusos" (párrs. 86-87).[82] Más recientemente, en su decisión de *Digital Rights Ireland Ltd*,[83] la Gran Sala del Tribunal de Justicia de la Unión Europea sostuvo que, a pesar de que la retención de datos de telecomunicaciones en la Directiva perseguía el objetivo legítimo de la lucha contra "delitos graves", la naturaleza de la obligación implicaba "una injerencia en los derechos fundamentales de la práctica totalidad de la población europea",[84] incluidas "las personas para las que no hay pruebas que sugieran que su conducta podría tener una vinculación, incluso indirecta o remota, con un delito grave".[85]

Por su propia naturaleza, la vigilancia masiva no conlleva ningún tipo de dirección o de selección, y mucho menos ninguna obligación de las autoridades de demostrar una sospecha razonable o causa probable.[86] En consecuencia, la vigilancia masiva es inevitablemente desproporcionada como una simple cuestión de definición. Los Principios reflejan las antes mencionadas normas internacionales en los epígrafes de "necesidad", "idoneidad" y "proporcionalidad".

En cuanto a la vigilancia específica, los Principios exponen los elementos que deben reconocerse ante una autoridad judi-

cial competente previo a la vigilancia. Los elementos requieren restricciones minuciosas sobre la información a la que se accede, así como los límites sobre el uso y retención. Como se verá más adelante, es importante destacar que esta disposición requiere la intervención de una Autoridad Judicial Competente.

PRINCIPIOS 6, 7: AUTORIDAD JUDICIAL COMPETENTE & DEBIDO PROCESO

Vigilancia y previa autorización judicial

Como se señaló anteriormente, los Principios exigen que todas las decisiones relacionadas con la vigilancia de las comunicaciones se hagan por una autoridad judicial competente que actúe con independencia del gobierno y de acuerdo con el debido proceso de ley. Esto refleja el requisito básico del derecho internacional de los derechos humanos de que el uso legítimo de las facultades de vigilancia de los funcionarios no solo debe ser necesario y proporcional, sino también debe contar un seguimiento independiente con estrictas salvaguardas contra el abuso.[87] Como sostuvo el Tribunal Europeo de Derechos Humanos en su decisión de 1979 en *Klass v. Alemania*:[88]

> El Estado de Derecho implica, *inter alia*, que una injerencia de los organismos del poder ejecutivo en los derechos de un persona debe ser objeto de un control efectivo que normalmente debería estar asegurada por el poder judicial, al menos en última instancia, ofreciendo el control judicial las mejores garantías de independencia, imparcialidad y juicio justo.

Aunque el Tribunal de Justicia en *Klass* acordó que "en principio es conveniente encomendar el control de supervisión a un juez", no fue tan lejos como para sostener que se requiere autorización judicial previa en todos los casos, en tanto que el organismo de autorización pertinente fuese "suficientemente independiente" de "las autoridades que realizan la vigilancia" para "ofrecer una decisión objetiva" y también estuviese invest-

ido "con facultades y competencias suficientes para ejercer un control efectivo y continuo".[89] En los casos siguientes, sin embargo, el Tribunal de Justicia ha puesto de manifiesto la conveniencia de la autorización judicial para el uso de la vigilancia legal. En un caso en 1999, por ejemplo, el Tribunal señaló que:

> Por no decir más, es sorprendente que [la] labor [de autorizar intercepciones] deba ser asignado a un funcionario del departamento legal de la Oficina de Correos, que pertenece al poder ejecutivo, sin la supervisión de un juez independiente, sobre todo en esta sensible área de las relaciones confidenciales entre un abogado y sus clientes, que se refieren directamente a los derechos de la defensa.[90]

Los Principios, sin embargo, reflejan la opinión de que la autorización judicial previa de las facultades de vigilancia no es solo deseable, sino esencial. Esto se debe a que ninguno de los otros dos poderes del Estado es capaz de proporcionar el necesario grado de independencia y objetividad como para evitar el abuso de las facultades de vigilancia. La opinión de la Corte en *Klass*—que la supervisión de un órgano parlamentario podría ser lo suficientemente independientes—ya no parece sostenible, en particular a raíz de los atentados del 11S, pues, los legisladores se han mostrado demasiado dispuestos a sacrificar los derechos individuales en nombre de la promoción de la seguridad. En el caso de la rama ejecutiva, los peligros son aún más agudos. En el Reino Unido, por ejemplo, los mismos ministros del gobierno que son responsables por las actividades de los servicios de inteligencia también son responsables de autorizar las órdenes de interceptación, y lo hacen con el asesoramiento de esos organismos—una salvaguarda poco aceptable contra posibles abusos.

Además, en agosto de 2012, el Tribunal Constitucional de Corea del Sur rechazó la recopilación de datos de suscriptores ante la ausencia de una autorización judicial previa, sobre la

base de que esto equivalía a "tratarlos como delincuentes en potencia".[91] Esto fue ratificado por la Comisión Nacional de Derechos Humanos coreana, que decidió, en abril de 2014, que la ausencia de cualquier requerimiento de autorización judicial previa para el acceso a los datos recogidos por la policía viola el derecho internacional de los derechos humanos.[92] También es destacable que, entre sus recientes recomendaciones en relación con la vigilancia de la NSA, el Comité de Derechos Humanos de las Naciones Unidas exhortó al gobierno de EE.UU. a facilitar "la intervención judicial en [la] autorización o supervisión de medidas de vigilancia".[93] Por estas razones, los Principios respaldan la opinión de que solo un juez ofrece las suficientes garantías de independencia e imparcialidad para garantizar que las facultades de vigilancia se ejerzan de una manera que sea a la vez necesaria y proporcionada.

En la práctica, sin embargo, tener un juez de vigilancia decidiendo en temas de vigilancia no es suficiente para proteger los derechos fundamentales. Los Principios también dejan en claro la importancia de contar con jueces que están 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. Del mismo modo, los jueces que autoricen deben disponer de recursos suficientes para llevar a cabo las funciones que se les asignen, incluyendo la supervisión continua de todas las actividades de vigilancia autorizada.

Uno de los defectos principales de los modelos existentes de autorización judicial previa es el hecho de que las solicitudes de vigilancia se da a través de un procedimiento *ex parte* y sin previo aviso.[94] En términos prácticos, esto significa que muy pocas solicitudes son rechazadas. Sin duda, un factor significativo es la falta de cualquier tipo de procedimiento contencioso, de modo que los intereses de la persona objeto de la vigilancia no están representados de manera efectiva. En algunas juris-

dicciones, sin embargo, se han adoptado diversos mecanismos con el fin de tratar de introducir elementos contenciosos en el procedimiento. Un ejemplo de ello es la Supervisión del Interés Público de Queensland, en el que se asigna automáticamente a un abogado para representar los intereses de la persona afectada cuando se presenta una solicitud de vigilancia.[95] Otras instancias podrían incluir el nombramiento de un defensor especial (tal como se utiliza en los procedimiento de inmunidad por razones de interés público en el Reino Unido y en otros lugares) con el fin de representar los intereses de la persona que no tiene conocimiento de la solicitud.[96] Estos modelos están lejos de ser perfecto, pero representan intentos de buena fe de cuadrar el círculo en relación a la impugnación efectiva de decisiones de vigilancia encubierta.

El otro principio relevante en este contexto es Debido Proceso. Es decir, las decisiones de vigilancia no solo deben hacerse de acuerdo con la ley, sino también de una manera compatible con los derechos fundamentales de la persona afectada.[97] La autorización judicial previa es una garantía importante a este respecto, pero muchos países establecen que en casos de emergencia las facultades de vigilancia a veces pueden ser usadas. Por lo tanto, los Principios exigen que la autorización retroactiva debe solicitarse dentro de un período de tiempo razonable y factible con el fin de prevenir abusos de las facultades de emergencia. También requieren la posterior notificación de las decisiones de vigilancia (*véase* la Notificación del Usuario) para que las personas afectada tengan la oportunidad de impugnar la legalidad, necesidad y proporcionalidad de cualquier decisión sobre vigilancia. En ausencia de un procedimiento contencioso efectivo en la obtención de la autorización de la vigilancia, los Estados también deben considerar la introducción de mecanismos internos adecuados que permitan solicitudes *ex parte* de manera que la vigilancia pueda ser adecuadamente cuestionada antes de que se conceda la autorización.[98]

Intercambio de datos, supervisión judicial y autorización previa

Entre los muchos problemas causados por la recogida masiva y la retención de los datos de las comunicación privadas es la falta de controles adecuados sobre la distribución posterior de estos datos por los diferentes organismos gubernamentales, así como entre los diferentes gobiernos. Un ejemplo reciente es la manera en que los datos de la NSA—supuestamente recolectados con el fin de contrarrestar las amenazas a la seguridad nacional—han sido utilizado por los organismo que combaten el tráfico de drogas, la policía y con fines de investigación fiscal.[99] De hecho, estos problemas pueden surgir incluso dentro de los diferentes departamentos del mismo organismo, por ejemplo, el intercambio de datos entre la rama de control general de los ingresos fiscales de Canadá y sus unidades de investigaciones criminales—divisiones que operan bajo restricciones legales muy diferentes, reflejando diferentes estándares, que son aplicables en procedimientos civiles y penales.

Este problema del intercambio irrestricto de datos debe abordarse no solo a través de las adecuadas medidas de protección de datos, sino también, según el caso, por medio de la supervisión judicial de las órdenes de registro de forma tal que el tribunal pueda evaluar si es necesario y proporcionado que la información solicitada sea compartida con otros organismos públicos. Esta cuestión también es abordada en el principio de proporcionalidad.

PRINCIPIO 8: NOTIFICACIÓN DEL USUARIO Y EL DERECHO A UN RECURSO EFECTIVO

En el derecho internacional de los derechos humanos, los principios de notificación del usuario y transparencia se entienden mejor en el marco del derecho a la intimidad y también como parte del derecho a un recurso efectivo y a un juicio justo.[100] Es fundamental en cualquier sistema efectivo de justicia que donde haya

> derecho exista un remedio (*ubi jus ibiremedium*).[101] Sin embargo, es imposible que una persona impugne efectivamente la interferencia de un gobierno en su vida privada si no sabe si ha sido víctima. En líneas generales, la falta de transparencia respecto a la aplicación de las leyes que rigen la vigilancia encubierta puede impedir el control democrático significativo de esas leyes, permitiendo que los organismos de inteligencia sean sus propios legisladores.

Desafortunadamente, a pesar de que la legislación europea exige la notificación del usuario en el contexto de la protección de datos en general,[102] el Tribunal Europeo de Derechos Humanos no ha encontrado que tal notificación sea un requisito necesario en los casos de vigilancia encubierta.[103] De hecho, en el caso de 1979 de *Klass v. Alemania*, el Tribunal reconoció que la falta de un requisito posterior a la notificación significa que las decisiones de vigilancia no son justiciables en lo que respecta a la persona afectada:

> [L]a naturaleza y la lógica de la vigilancia secreta dictan que no solo la vigilancia propiamente dicha, sino también la revisión que la acompaña deban ser efectuadas sin el conocimiento del individuo. En consecuencia, puesto que el individuo necesariamente estará impedido de buscar un remedio efectivo por su propia voluntad o de tomar parte directa en cualquier procedimiento de revisión, es esencial que los procedimientos establecidos ofrezcan garantías adecuadas y protecciones equivalente que salvaguarden los derechos de la persona.

En un caso posterior, en 2007, el Tribunal sugirió que "tan pronto como la notificación pueda realizarse sin poner en peligro el objetivo de la vigilancia y tras su conclusión, se debe proporcionar información a las personas afectadas",[104] sin llegar a reconocer que la notificación era un requisito necesario de las legislaciones de vigilancia en general. Sin embargo, en los 35 años

transcurridos tras la decisión del Tribunal en *Klass,* ha quedado claro que no existen "garantías adecuadas y equivalentes" a la notificación efectiva del usuario. En el Reino Unido, por ejemplo, la gran mayoría de las decisiones de vigilancia bajo la Ley de regulación de las facultades de investigación se han hecho sin que medie ninguna autorización judicial previa o la posterior supervisión judicial.[105] Como consecuencia del razonamiento del Tribunal en *Klass*, muchas de las decisiones de vigilancia han escapado del control público y de la supervisión judicial efectiva.

El desafortunado planteamiento adoptado por el Tribunal Europeo de Derechos Humanos en *Klass* es, además, claramente contrario a la experiencia de esas jurisdicciones en las que, por muchos años, han operado los requisitos de notificación del usuario tras la conclusión de la vigilancia. En Canadá, por ejemplo, la legislación limita el plazo de vigilancia e impone la obligación de notificar a la persona bajo vigilancia dentro de los 90 días desde la fecha en que termine la vigilancia, prorrogables a un máximo de tres años.[106] Por esta razón, los Principios enfatizan en la necesidad de la notificación a la primera ocasión, estableciendo una lista exhaustiva de las circunstancias que pueden justificar un retraso—solo cuando la notificación ponga en grave peligro la finalidad de la vigilancia o exista un riesgo inminente de peligro para la vida humana. También exigen que cualquier retraso sea examinado por una autoridad judicial competente, lo que implica que en ocasiones la notificación pueda ocurrir incluso antes de que se considere "disipado" un riesgo a los fines por los que la vigilancia se autorizó.[107] Esto se hace porque, con frecuencias, las investigaciones se extienden indefinidamente sin que pueda asegurarse su legitimidad. De hecho, algunas leyes de vigilancia expresamente reconocen esto.

En la práctica, cualquier sistema de notificación del usuario inevitablemente es vulnerable a las solicitudes *ex parte* de las organismos gubernamentales con el fin de demorar o impedir la notificación en casos particulares. La naturaleza de este tipo

de solicitudes significa que se les pedirá a los tribunales que determinen la necesidad de mantener el secreto sobre la base de información parcial presentada por las autoridades. Para que el principio de la notificación del usuario sea efectivo, le corresponde a las legislaturas diseñar mecanismos que en lo posible permitan los procedimiento contenciosos en las decisiones sobre vigilancia como anteriormente se discutió en la sección sobre la autorización judicial previa.

Por último, es importante tener en cuenta que la notificación del usuario y la transparencia sirven intereses distintos: el primero se refiere a proveer información suficiente sobre una decisión de vigilancia a la persona afectado para que pueda impugnar o buscar remedios efectivamente; la segunda tiene por objeto garantizar que el público en general tenga información suficiente para evaluar si las leyes que rigen la vigilancia están funcionando con efectividad, en concreto, si existen garantías suficientes para el ejercicio del derecho a la intimidad de las personas. Esto se discute con más detalles en la siguiente sección.

Así pues, el principio de la notificación del usuario requiere la notificación con tiempo suficiente para permitir la impugnación y solo autoriza un retraso en pocas circunstancias autorizadas por una autoridad judicial competente, para garantizar que el retraso se justifique y no sea extienda más allá de lo estrictamente necesario para proteger una investigación o para proteger contra un riesgo a la vida humana.

PRINCIPIOS 9, 10: TRANSPARENCIA & SUPERVISIÓN PÚBLICA

El principio de supervisión pública está estrechamente relacionado con, pero distinto a, la cuestión de los recursos en casos individuales; se refiere a la importancia de la transparencia para la democracia en general. En una democracia, la ciudadanía participa en el desarrollo de las leyes a través de

sus representantes electos. Por tanto, es esencial que tengan información suficiente sobre cómo esas leyes se están aplicando con el fin de tomar decisiones informadas, ya sea en las urnas o cuando deliberan con otros sobre asuntos de política pública.[108] También, en un democracia es importante que aquellos funcionarios públicos a quienes se les ha confiado la facultad de llevar a cabo la vigilancia 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.[109]

La necesidad de garantizar la transparencia democrática es aún más importante en los casos en que, por razones operativas, aspectos del sistema se mantienen en secreto y no están sujetos a supervisión judicial. Como sostuvo el Tribunal Europeo de Derechos Humanos en *Klass*, "las facultades de vigilancia secreta de la ciudadanía, que caracterizan la forma como lo hacen los Estados policiales, son solo tolerables bajo la Convención en la medida estrictamente necesaria para salvaguardar las instituciones democráticas".[110] Esto da lugar a dos requisitos fundamentales: en primer lugar, cualquier sistema normativo que rija la vigilancia no solo debe imponer restricciones firmes a cualquier margen de discreción de los funcionarios públicos, sino también las leyes en cuestión debe ser "suficientemente clara en sus términos para proporcionar a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en que las autoridades públicas están facultadas a recurrir a esta interferencia secreta y potencialmente peligrosas para el derecho al respeto de la vida privada y la correspondencia".[111] En segundo lugar, las leyes también deben ofrecer garantías suficientes para evitar el riesgo de abuso de poder o arbitrariedades.[112]

Como también ha señalado el Comité de Derechos Humanos de las Naciones Unidas, es tan importante que el Estado proporcione garantías sobre el papel, como que realmente lleve a cabo controles continuos para verificar si estas medidas de

seguridad funcionan en la práctica. El manifiesto fracaso en dicho control en EE.UU., el Reino Unido y en otros lugares, es una de las características más notables de los resultados de las revelaciones de Snowden.[113] Los Principios reflejan adecuadamente el recordatorio del Comité de Derechos Humanos sobre la importancia de que funcionen apropiadamente los órganos de monitoreo y supervisión.[114]

El control público también exige a los gobiernos proporcionar al público información suficiente, clara y precisa para permitir una evaluación seria de la necesidad y proporcionalidad del uso de las facultades de vigilancia en la práctica.[115] Estadísticas sin sentido y opacas no pueden servir para este propósito. Aunque algunas cuestiones operativas pueden permanecer en secreto, en una sociedad democrática esto no debe dar lugar al uso de las facultades de vigilancia sin que haya rendición de cuenta, sin control democrático y externo.

Por lo cual, los Principios contienen requisitos relativamente detallados y requieren de supervisión independiente. También prohíben expresamente la interferencia con los proveedores de servicios que publican información como parte de sus propios esfuerzos de transparencia.

PRINCIPIO 11: INTEGRIDAD DE LAS COMUNICACIONES & SISTEMAS

El derecho a la intimidad conlleva el derecho de las personas a construir medios para comunicarse con otros sin intromisiones externas. El deber de los gobiernos de respetar la privacidad de las comunicaciones también impone una obligación de respetar la integridad de todos y cada uno de los sistemas utilizados para transmitir comunicaciones privadas. Sin embargo, una de las revelaciones más significativas de este año ha sido el grado en que la NSA, el GCHQ y otros, aparentemente han trabajado para minar la infraestructura global de las comunicaciones, obteniendo claves privadas cifradas a través de

servicios comerciales, instalando puertas traseras en herramientas de seguridad, o socavando los estándares criptográficos de clave de millones de personas en todo el mundo.[116] En abril de 2013, el Relator Especial de las Naciones Unidas para la Libertad de Expresión señaló que "la seguridad y el anonimato de las comunicaciones también son socavadas por leyes que limitan el uso de herramientas para la protección de la intimidad que pueden ser usadas para proteger las comunicaciones, como el cifrado".[117] En consecuencia, recomendó que:

> Las personas deben tener libertad de usar cualquier tecnología que elijan para asegurar sus comunicaciones. Los Estados no deben interferir con el uso de tecnologías de cifrado, ni obligar a entregar las claves de cifrado.

De esta manera, el Principio 11 refleja el requisito básico de que toda interferencia con la privacidad de las comunicaciones no solo debe ser legal, sino también proporcionada. Del mismo modo que no sería razonable que los gobiernos insistan en que todos los residentes de una casa dejen sus puertas abiertas en caso de que policía tenga que registrar una propiedad en particular, o exigir a todas las personas que instalen cámaras de vigilancia en sus casas sobre la base de que podría ser útil para futuros enjuiciamientos, es igualmente desproporcionado que los gobiernos interfieran con la integridad de las comunicaciones con el fin de facilitar las investigaciones o requerir la identificación de los usuarios como condición previa para la prestación de servicios o la retención de todos los datos de clientes.[118] Cabe destacar que, en sus recientes observaciones sobre el Cuarto Informe Periódico de Estados Unidos, llevada a cabo como parte de su Examen Periódico Universal, el Comité de Derechos Humanos reconoció que, en relación con los problemas inherentes a los regímenes de retención de datos, Estados Unidos deben, entre otras cosas, "abstenerse de imponer la retención obligatoria de datos por terceros".[119] De esta manera, la suposición inherente detrás de tal interferencia—que todas

las comunicaciones son potencialmente criminales—es contraria a la presunción de inocencia, un requisito fundamental del derecho internacional de los derechos humanos.[120]

PRINCIPIO 12: GARANTÍAS PARA LA COOPERACIÓN INTERNACIONAL

Cada vez con mayor frecuencia las actividades de vigilancia estatal de las comunicaciones abarcan límites territoriales. Además de la colaboración mundial para la vigilancia de las redes de comunicaciones llevada a cabo por muchas organismos de inteligencia extranjeros y discutido anteriormente, una mayor cooperación entre los gobiernos también incluye la cooperación más formal entre los organismos encargados de hacer cumplir la ley, incluso a través de los Tratados de Asistencia Legal Mutua (MLATs, por sus siglas en inglés).

La cooperación internacional entre gobiernos plantea dudas en cuanto a cómo y cuándo los Estados pueden ser responsables bajo el derecho nacional e internacional por sus actividades de vigilancia, que pueden tener un impacto mucho más allá de sus propias fronteras. Una cuestión es el grado en que los Estados pueden ser "extraterritorialmente" responsables de violaciones de los derechos humanos en el extranjero, por ejemplo, la vigilancia de las comunicaciones privadas en otros países. No obstante, es importante tener en cuenta que la tecnología actual permite a los Estados monitorear una gran cantidad de tráfico internacional desde sus propias fronteras. Por tanto, es imperativo considerar la cuestión de la jurisdicción en el derecho internacional de los derechos humanos y las diferentes formas en que un Estado puede ser considerado responsable de sus actos, incluso cuando sus efectos ocurren más allá de sus fronteras.[121]

Un área concreta de preocupación es la práctica no autorizada de los Estados de "extraer" datos de los servidores en otros países, sin el consentimiento o conocimiento de esos

gobiernos. Según se desprende de las revelaciones de Snowden, por ejemplo, las autoridades estadounidenses pueden exigir a las empresas con sede en EE.UU. que entreguen los datos de los servidores de su propiedad que operan en otros países y también pueden solicitar a estas empresas que no informen sobre la obligación de divulgación de los datos a las autoridades de los países de donde extraen los datos, a las entidades cuyos datos están entregando o, de hecho, a los titulares de los datos.

No solo este tipo de prácticas manifiestamente infringen los requisitos de la legislación nacional de protección de datos de los países de donde extraen los datos, sino también violan el principio fundamental del derecho internacional de que un Estado "no puede adoptar medidas en el territorio de otro Estado mediante la aplicación de leyes nacionales, sin el consentimiento de este último".[122] Como señaló la Comisión de Derecho Internacional:[123]

> En cuanto a la jurisdicción para hacer cumplir leyes, un Estado no puede hacer valer su derecho penal, es decir, *investigar* delitos o detener a sospechosos, en el territorio de otro Estado sin el consentimiento del otro Estado. [Énfasis añadido].

El canal adecuado para la cooperación internacional en estos asuntos es a través de los MLATs. En este contexto, es altamente polémica una disposición del Convenio del Consejo de Europa contra la *Ciberdelicuencia* que sugiere que la recopilación de datos transnacional por los organismos de aplicación de la ley podría ser posible con el consentimiento, no del Estado de destino, sino con "el consentimiento legal y voluntario de la persona que tiene la autoridad legal para divulgar los datos del [organismo del orden público que lo solicita]" (Art. 32(b)). En la reciente Conferencia Octopus sobre Cooperación contra el Delito Cibernético (Estrasburgo, 4-6 de diciembre de 2013), se acordó estudiar la formulación de un nuevo protocolo a la *Convención contra la Ciberdelicuencia* o al *Convenio*

del Consejo de Europa sobre Protección de Datos (o un tratado nuevo y separado) para abordar esta cuestión.[124] Esto confirma que el acceso transnacional a los datos, y la "extracción" de los datos en otros países sin el consentimiento de éstos, se considera contraria al derecho internacional público, y que el controvertido artículo de la *Convención contra la Ciberdelincuencia*, por sí mismo, no expresa tal consentimiento.

PRINCIPIOS 13: GARANTÍAS CONTRA EL ACCESO ILEGÍTIMO

El último principio se basa en una serie de normas internacionales relacionadas con la protección al derechos a la intimidad. En primer lugar, el deber de los gobiernos de impedir la vigilancia ilegal por medio de sanciones penales y civiles refleja las exigencias del derecho internacional de los derechos humanos de proteger a los individuos de violaciones a su intimidad, no solo por el Estado, sino también por particulares.[125] En segundo lugar, la necesidad de que las vías de reparación reflejen asimismo las normas internacionales relativas al derecho a un recurso efectivo por violaciones de los derechos humanos.[126]

En tercer lugar, la necesidad de proporcionar una protección efectiva a los denunciantes ('*whistleblowers*') nace de varios instrumentos internacionales, incluido el artículo 19 del PIDCP y la Convención de las Naciones Unidas contra la Corrupción (2005).[127] Varios expertos de las Naciones Unidas han hecho hincapié en la importancia que tienen los denunciantes que revelan actos ilegales o violaciones de derechos humanos por parte de las autoridades públicas. En particular, el Relator Especial de Naciones Unidas para la Libertad de Opinión y de Expresión ha subrayado en numerosas ocasiones que la denuncia de irregularidades es un aspecto importante del derecho a la libertad de expresión.[128] Más específicamente, el Relator Especial de la Naciones Unidas para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo ha declarado que los denunciantes

son cruciales para "romper los anillos ilegales de información secreta" dentro de los organismos de inteligencia y de seguridad que cometen violaciones de derechos humanos, y que en estos casos, el interés público en revelar la información prevalece sobre el interés en mantenerla secreta.[129] Además, ha declarado que los denunciantes deben ser protegidos de represalias legales y acciones disciplinarias por desvelar información no autorizada, siendo necesarios mecanismos para su protección. Varios instrumentos, incluidos los *Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y Acceso a la Información*[130] y los *Principios de Tshwane sobre la Seguridad y Nacional y el Derecho a la Información*[131] elaboran más a fondo los tipos de recursos y protecciones que deberían recibir los denunciantes.[132]

En cuarto lugar, la obligación para que sean inadmisible las pruebas obtenidas de manera incompatible con los Principios subraya la necesidad de garantizar que todos los organismos gubernamentales actúen de conformidad con los derechos fundamentales, que a su vez es un requisito básico del Estado de Derecho. En algunos países, la regla de exclusión en contra del uso de pruebas obtenidas ilegalmente es absoluta; lo que refleja un principio constitucional fundamental, *véase*, por ejemplo, la doctrina del "fruto del árbol envenenado" bajo la legislación estadounidense.[133] En otras jurisdicciones, la regla no es necesariamente de carácter absoluto,[134] sino que los medios ilegales por los que se obtuvo la evidencia es siempre un factor importante que tienen en cuenta los tribunales a la hora de determinar si la persona ha recibido un juicio justo.[135]

En quinto y último lugar, la necesidad de destruir o devolver el material obtenido como resultado de la vigilancia refleja las consolidadas leyes de protección de datos en una amplia gama de jurisdicciones.

NOTAS AL FIN

1 Para más información sobre el proceso de consulta, *véase* Privacy International, *Towards International Principles on Communication Surveillance*, en donde se hace referencia a una reunión de expertos en Bruselas en octubre de 2012, 21 de noviembre de 2012. Disponible en **https://www.privacyinternational.org/blog/towards-international-principles-on-communications-surveillance.**. Este encuentro fue seguido por una reunión organizada por la Electronic Frontier Foundation en Río de Janeiro, Brasil, en diciembre de 2012, que contó con la participación del Relator Especial de las Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Frank La Rue. Véase el documento de las Naciones Unidas A/HRC/23/40, párr. 10. La Electronic Frontier Foundation, Privacy International y Access lanzaron una consulta mundial que concluyó en enero de 2013. Además, trabajaron en la revisión del texto, hasta julio de 2013, junto con varias organizaciones no gubernamentales, abogados penalistas, abogados de derechos humanos y defensores del derecho a la intimidad.

2 El texto completo de los *Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones* está disponible en **https://en.necessaryandproportionate.org/text**.

3 La lista completa de los firmantes está disponible en: **https://en.necessaryandproportionate.org/signatories**.

4 *Informe y recomendaciones del Grupo de Revisión del Presidente sobre inteligencia y tecnologías de las comunicaciones. Libertad y seguridad en un mundo cambiante*, 12 de diciembre de 2013, nota 120. Disponible en **http://whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf**.

5 *Informe Anual de la Comisión Interamericana de Derechos Humanos*, 31 de diciembre de 2013. Disponible en **http://www.oas.org/en/iachr/docs/annual/2013/informes/LE2013-eng.pdf**.

6 *Necesarios y proporcionados*, Noticias. Disponible en: **https://en.necessaryandproportionate.org/news**.

7 Estamos muy agradecidos a todos los que nos ayudaron con la investigación y redacción de este documento. En particular agradecemos a Douwe Korff, Profesor de Derecho Internacional de los Derechos Humanos, por la preparación de una versión anterior del documento, y a Cindy Cohn, Gabrielle Guillemin, Tamir Israel, Dr. Eric Metcalfe y Katitza Rodríguez por sus posteriores contribuciones. Extendemos unas palabra de agradecimiento especial a Access, Privacy International, Asociación por los Derechos Civiles, Comisión Colombiana de Juristas, Fundación Karisma, Human Rights Information and Documentation System – HURIDOCS, El Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, y Open Net Korea por revisar y compartir recursos bibliográficos. Aunque intentamos promover una amplia consulta, agradeceríamos recibir aportes adicionales de expertos en los derechos

africano y de Europa del Este, tanto de organismos nacionales como regionales, que no están representados con tanta fuerza en esta primera versión del documento.

8 Para un análisis académico más profundo y más referencias sobre la jurisprudencia del Comité de Derechos Humanos y otras fuentes, *véase* Martin Scheinin & Mathias Vermeulen, "Unilateral Exceptions to International Law: Systematic legal Analysis and Critique of Doctrines that seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism," sección 3.7 en *Denial of Extraterritorial Effect of Human Rights (Treaties)*. Disponible en **http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf.**

9 Para un ejemplo, *véase* G. Greenwald & E. MacAskill, "Boundless Informant: the NSA's Secret Tool to Track Global Surveillance Data," *The Guardian*, 11 de junio de 2013. Disponible en **http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining**; La NSA es quizás el ejemplo más claro del nivel de alcance y amplitud que tiene un organismo de inteligencia extranjero de aprovechar las redes interconectadas y espiar a cualquier persona alrededor del mundo. Sin embargo, muchos de las otras naciones partes de los *Five Eyes* están ubicadas estratégicamente de manera que complementen el alcance que tiene la NSA con la información en tránsito (o almacenada en) su propia zona de influencia. Por ejemplo, *véase* N. Hopkins, "Theresa May Warns Yahoo That Its Move to Dublin is a Security Worry," *The* Guardian, 20 de marzo de 2014. Disponible en **http://www.theguardian.com/technology/2014/mar/20/theresa-may-yahoo-dublin-security-worry**.

10 Privacy International, "Eyes Wide Open", Versión 1.0, 2013. Disponible en **https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf**.

11 *Véase*, por ejemplo, S. Ackerman & J. Ball, "Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ," *The Guardian*, 28 de febrero de 2014. Disponible en **http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo**: "Programas como el *Optic Nerve*, que recopila información en masa de identificaciones de usuarios en gran parte anónimas, no son capaces de filtrar información de nacionales del Reino Unido o de Estados Unidos."; John Foster, Jefe del Centro de Seguridad de las Comunicaciones de Canadá (CSEC, por sus siglas en inglés), Testimonio ante el Comité Permanente del Senado sobre Seguridad Nacional y Defensa, 41ª Parlamento , 2º Período de Sesiones 2013-14, 3 de febrero de 2014, disponible en **http://www.parl.gc.ca/content/sen/committee/412/SECD/pdf/02issue.pdf**, p. 2-71: "Vamos a mantener los metadatos, pues, cuando las comunicaciones transitan en las redes, las comunicaciones de extranjeros y canadienses quedan mezcladas…Cuando recopilas metadatos es imposible. Todo se entremezcla, y las mismas redes son usadas por los buenos ciudadanos y los terroristas. Así que, cuando las recopilamos, en ese momento no tenemos forma de hacer distinciones hasta que nos fijamos en ellas, y es entonces que las usamos."

12 Comité de Derechos Humanos de las Naciones Unidas (CDH), Comentario General no. 31 [80], Naturaleza de la obligación jurídica general impuesta a los Estados Partes en el Pacto, 26 de mayo de 2004, CCPR/C/21/Rev.1/Add.13. Disponible en **http://www.refworld.org/docid/478b26ae2.html** [consultado el 18 de mayo de 2014].

13 Por ejemplo, de conformidad con la Convención Interamericana de Derechos Humanos, los Estados deben: "230. [A]bstenerse de realizar acciones o favorecer prácticas que de cualquier manera se encuentren dirigidas, directa o indirectamente, a crear situaciones que, *de iure* o *de facto*, discriminen o excluyan arbitrariamente a ciertos grupos o personas en el goce o ejercicio del derecho a la libertad de expresión. Asimismo, deben adoptar medidas positivas (legislativas, administrativas o de cualquier otra naturaleza) para revertir o cambiar situaciones discriminatorias existentes que comprometan el goce y ejercicio efectivo del derecho a la libertad de expresión de ciertos grupos, en condiciones de igualdad y no discriminación." *Véase* CIDH. *Informe Anual 2008*. Informe Anual de la Relatoría Especial para la Libertad de Expresión. Capítulo III (Marco Jurídico Interamericano del Derecho a la Libertad de Expresión). OEA/Ser.L/V/II.134 Doc. 5 rev. 1, 25 de febrero de 2009, párr. 230. Disponible en **http://cidh.oas.org/annualrep/2008eng/Annual%20Report%202008-%20RELE%20-%20version%20final.pdf.** *Véase* también Comisión Interamericana de Derechos Humanos. Relatoría Especial para la Libertad de Expresión. *Libertad de Expresión e Internet*. Registros oficiales de la OEA; OEA/Ser.L/V/II. CIDH/RELE/INF.11/13, 31 de diciembre de 2013, página 9. Disponible en **http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf**.

14 Pacto Internacional de Derechos Civiles y Políticos (PIDCP), artículo 2(1); Resolución de la Asamblea General de las Naciones Unidas 2200A (XXI); el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, modificado por los Protocolos no. 11 y no. 14, Roma, 4.XI.1950 (Convenio Europeo de Derechos Humanos o CEDH), artículo 1; Convención Americana sobre Derechos Humanos, OEA Serie de Tratados No. 36, 22 de noviembre de 1969, (CIDH), artículo 1.1.; la Carta Africana de Derechos Humanos y de los Pueblos, OUA Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) (CADHP), establece que "Los Estados miembros de la Organización de la Unidad Africana firmantes de la presente Carta reconocerán los derechos, deberes y libertades reconocidos en el presente Capítulo y se comprometerán a adoptar medidas legislativas o de otra índole para darles efecto" (artículo 1).

15 42 EHRR 1 (2005).

16 48 EHRR 1 (2009).

17 No. 54934/00, 29 de junio de 2006.

18 El gobierno alemán había argumentado que la aplicación era incompatible *ratione personae* sobre la base de que el "control de las telecomunicaciones

desde el extranjero" era un "acto extraterritorial", por lo tanto, fuera de la jurisdicción de Alemania bajo el artículo 1 del CEDH. La TEDH, sin embargo, se negó a archivar el recurso por este motivo (*véase* el párr. 72 de la Decisión), aunque en última instancia sí archivó la demanda por otros motivos.

19 Casos. no. 52/1979 y 56/1979, ambas del 29 de julio de 1981, párrs. 12.3 y 10.3 respectivamente. *Véase también* las Observaciones Finales del Comité sobre los Informes de Israel de 1998 y 2003, mencionados en Scheinin y Vermeulen, *op. cit.* (nota 8, *supra*), p. 37, nota 81. *Véase* también la Observación General no. 31, párr. 10.

20 TEDH, *Issa y otros v. Turquía*, sentencia de 16 de noviembre de 2004, firme desde el 30 de marzo de 2005, párr. 68.

21 *Véase* Observaciones Finales de 2006 del CDH sobre el Informe de EE.UU. bajo el PIDCP; CCPR/C/USA/CO/3, párr. 10, y el Informe de 2011 de los EE.UU. a la CDH, CCPR/C/USA/4, párr. 505.

22 *Right to Privacy in the Digital Age – U.S. Redlines*. Disponible en **http://columlynch.tumblr.com/post/67588682409/right-to-privacy-in-the-digital-age-u-s**.

23 *Human Rights Committee considers report of the United States*, 14 de marzo de 2014. Disponible en **http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=14383&LangID=E**.

24 Para más información, *véase* Electronic Frontier Foundation & Human Rights Watch, "Joint Submission to the Human Rights Committee," 14 de febrero de 2014. Disponible en **https://www.eff.org/files/2014/03/10/hrweffsubmission_on_privacy_us_ccpr_final.pdf**.

25 Asamblea General de las Naciones Unidas, *El derecho a la privacidad en la era digital*, noviembre de 2013, A/C.3/68/L.45. Disponible en **http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf.**.

26 Los "datos de las comunicaciones" (o "registro de las comunicaciones") pueden ser desagregados en diferentes categorías, por ejemplo, los "datos de suscriptor" y los "datos de tráfico". Nótese que los "metadatos" son usados más a menudo en leyes de casos de EE.UU. mientras que la legislación latinoamericana, europea y británica más frecuentemente se refiere a los "datos de las comunicaciones" (que tiene una definición estatutaria en el Reino Unido en la sección 21(4) de Ley de regulación de los poderes de investigación (RIPA, por sus siglas en inglés). Sin embargo, el término "metadato" es cada vez más usado en el Reino Unido y Europa: *véase,* por ejemplo, la Directiva Práctica 31B de las Reglas de Procedimiento Civil en Inglaterra y Gales en donde se define metadato como "dato sobre datos"; o la Regulación de Metadados *INSPIRE* (CE) No 1205/2008 de 3 de diciembre de 2008. Sir David Omand, el antiguo director del GCHQ, ha criticado públicamente la sugerencia de que los "metadatos", como se entienden en

la legislación de EE.UU., sea equivalente a la definición de los "datos de las comunicaciones" en RIPA. Sin embargo, en los actuales procedimiento ante el Tribunal de Poderes Investigativos en relación con PRISM y TEMPORA, el gobierno de Reino Unido no ha sugerido que cualquier información está cubierta por el término "metadato", que no solo está cubierto por la definición de los "datos de las comunicaciones".

27 En Corea, por ejemplo, el "dato de comunicación" o "metadato" así definido incluirá los "registros de las comunicaciones" disponibles a la policía solo a través de la aprobación del tribunal en la Ley de protección del secreto de las comunicaciones, y los "datos de comunicación", a disposición de la policía dentro de la discreción que tienen los proveedores de servicios en la Ley de negocio de las telecomunicaciones, es, de hecho, la información provista sobre los suscriptores tras inscribirse en los servicios de telecomunicaciones. El *Código Penal* de Canadá prohíbe la interceptación de las comunicaciones privadas, que se ha interpretado en general como aplicable a los contenidos, no a los metadatos (o a los "datos de transmisión"). La información de transmisión está constitucionalmente protegida y, por lo general, requiere de alguna forma de autorización judicial. El gobierno canadiense intentó introducir una nueva categoría de "información sobre los suscriptores" en la legislación, lo que hubiera obligado a las empresas de telecomunicaciones a revelar dicha información a petición de distintos organismos; sin embargo, esta legislación no fue aprobada (M. Geist, "Lawful Access is Dead (For Now): Government Kills Bill C-30," 12 de febrero de 2013. Disponible en **http://www.michaelgeist.ca/content/view/6782/125/**. La legislación de Estados Unidos también reconoce una categoría de "información sobre los suscriptores"; por ejemplo, en su régimen de la Carta de Seguridad Nacional, en donde se autoriza a la Oficina Federal de Investigaciones a exigirle a los proveedores de comunicaciones que identifiquen clientes (revelar nombres, direcciones, tiempo de servicio y la información de facturación): D. Doyle, "National Security Letters in Foreign Intelligence Investigations: A Glimpse at the Legal Background," *Congress Research Service*, 3 de enero de 2014. Disponible en: **https://www.fas.org/sgp/crs/intel/RS22406.pdf**.

28 Por ejemplo, la Agencia de Seguridad Nacional de EE.UU. ha estado recopilando todos los metadatos de todas las llamadas telefónicas de las compañías telefónicas estadounidenses bajo las órdenes de producción que han sido regularmente renovadas y emitidas por el Tribunal de Vigilancia de Inteligencia Extranjera (FISC, por sus siglas en inglés). Para una descripción del programa *véase* Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," 23 de enero de 2014, pp. 8 -10. En respuesta a las preocupaciones sobre el derecho a la intimidad, recientemente el presidente Obama anunció el cierre inminente del programa de adquisición de metadatos de la NSA: C. Savage, "Obama to Call for End to N.S.A.'s Bulk Data Collection," *New York Times*, 24 de marzo de 2014. Disponible en **http://www.nytimes.**

com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html. Un programa similar comprendía la producción periódica de todos los metadatos de Internet, pero se interrumpió en 2011: G. Greenwald & S. Ackerman, "NSA Collected US Email Records in Bulk for More than Two Years under Obama," *The Guardian*, 27 de junio de 2013. Disponible en http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

29 D. Gilbert, I.R. Kerr & J. McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunication Providers," 51 *Crim. L. Quart.* 469 (2006). Disponible en http://iankerr.ca/wp-content/uploads/2011/08/the_medium_and_the_message.pdf.

30 El equivalente del " *Pen Register*" en la legislación estadounidense o "grabadores numéricos" en otras jurisdicciones.

31 *Véase* la presentación de Peter Sommer, *Can we separate "comms data" and "content"—and what will it cost?*, en el evento de 2012 "Scrambling for Safety". Disponible en http://www.scramblingforsafety.org/2012/sf2012_sommer_commsdata_content.pdf.

32 Igualmente, el Grupo de Trabajo del artículo 29 ha dicho *"También es muy importante tener en cuenta que los metadatos producen información más fácilmente que el contenido real de nuestras comunicaciones"*; ***véase*** 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. disponible en WP215, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

33 *Véase* la Declaración del profesor Edward Felten, antiguo Director de Tecnología en la Comisión Federal de Comercio de los EE.UU., en un litigio en curso presentado en los EE.UU. por la Unión Americana de Libertades Civiles (ACLU, por sus siglas en ingés) en relación con las revelaciones de Snowden. Disponible en https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26 ACLU PI Brief - Declaration - Felten.pdf. *Véase* también el Informe de *Amici Curiae* de Expertos en Ciencias Informática y Datos en apoyo de la parte recurrente y revocatoria en *ACLU v. Clapper*, apelación ante el 2º Circuito. Disponible en https://www.eff.org/document/computer-scientists-amicus-aclu-v-clapper.

34 *Véase*, por ejemplo, *Katz v. United States,* 389 U.S. 347 (1967), en donde la Corte Suprema de EE.UU. sostuvo que la vigilancia del FBI de las llamadas realizadas desde una cabina telefónica equivalía a un "registro" bajo la Cuarta Enmienda.

35 *Smith v. Maryland*, 442 U.S. 735, 744 (1979**).** Como se describe más adelante, hasta tanto no existe protección constitucional en EE.UU., hay algunas protecciones legales bajo la legislación estadounidense para la información en manos de terceros, incluidos los metadatos, como el *Pen Register* y los

estatutos de rastreo. Esto es insuficientes bajo los Principios "Necesarias y Proporcionadas", dado que la corte emite una orden basada solo en que se demuestre "relevancia" de una investigación. *Véase* 8 U.S. Code 3123 (para datos de intercambio prospectivo) y 18 U.S. Code 2703 (c), (d) (para información almacenada en las comunicaciones que ya han tenido lugar).

36 Grupo de Revisión del Presidente, "Liberty and Security in a Changing World," diciembre de 2013, p. 121, citando los Principios. Disponible en **http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf**.

37 18 U.S. Code 3123 (para datos de intercambio prospectivo) y 18 U.S. Code 2703 (c), (d) (para información almacenada en las comunicaciones que ya han tenido lugar).

38 Ley de protección del secreto de las comunicaciones de Corea, Artículo 13. Disponible en **http://elaw.kiri.re.kr/en_service/lawPrint.do?hseq=21696.**.

39 *Véase*, por ejemplo, *Malone v. United Kingdom* (1985) 7 EHRR 14, párr. 84.

40 *Véase*, en particular, Grupo de Trabajo del artículo 29, *Opinión 4/2007 sobre el concepto de "datos personales",* 20 de junio de 2007, WP136. Disponible en **http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf**. *Véase* también Grupo de Trabajo del artículo 29, *Opinión 04/2014 sobre la 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/opinion-recommendation/files/2014/wp215_en.pdf**.

41 *Véase: Digital Rights Irlanda v. Irlanda*, Asuntos acumulados C-293/12 y C-594/12, 8 de abril de 2014, párr. 25-31: "En tales circunstancias, a pesar de que, como se desprende..., la Directiva no permite que se mantenga el contenido de las comunicaciones o de la información consultada usando una red de comunicaciones electrónicas, no cabe excluir que la retención de los datos en cuestión pueda tener un efecto en el uso, por los suscriptores o usuarios registrados, de los medios de comunicación a que se refiere dicha Directiva y, en consecuencia, en el ejercicio de la libertad de expresión garantizada en el artículo 11 de la Carta. La retención de datos a los efectos de su posible acceso por las autoridades nacionales competentes...afecta directa y específicamente la vida privada y, en consecuencia, los derechos garantizados en el artículo 7 de la Carta. Por otra parte, esa retención de datos también se rige por el artículo 8 de la Carta, pues, es constitutivo del procesamiento de datos personales en el sentido de dicho artículo y, por tanto, necesariamente tiene que satisfacer los requisitos de protección de datos derivadas del artículo". *Véase* también el párr. 37: "Es preciso señalar que la interferencia causada por la Directiva 2006/24 a los derechos fundamentales establecidos en los artículos 7 y 8 de la Carta es, como ha señalado el Abogado General, en particular en los párrafos 77 y 80 de su Opinión, de amplio alcance y debe ser considerado como particularmente grave", haciendo

referencia a la Opinión del Abogado General sobre la cuestión (emitido el 12 diciembre de 2013). El artículo 7 de la *Carta de los Derechos Fundamentales de la UE* establece que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

42 Entre otras cosas, la ley de protección de datos de la UE está sujeta a un amplio principio de "equilibrio", que permite el tratamiento de datos personales (no sensibles) sin consentimiento y sin una base legal clara, siempre que los intereses de la persona afectada no "superen" los "intereses legítimos" del controlador, pero no está claramente definido lo que constituye intereses "sensibles" y "legítimos". Además, hay excepciones generales que permiten el procesamiento de datos personales sensibles, cuando sea "necesario" para proteger ciertos intereses más amplios, incluyendo la exclusión total para propósitos de "seguridad nacional".

43 *S y Marper v. Reino Unido*, 48 EHRR 50 (2009), párr. 121. El caso se refería a la retención "amplia e indiscriminada" de muestras de ADN de personas detenidas, sin imputación o condenada.

44 Asuntos acumulados C 293/12 y C 594/12, 8 de abril de 2014, párrs. 29 y 39. La Gran Sala del TJUE también encontró que la retención era una injerencia en el derecho a la protección de datos bajo del artículo 8 de la Carta (*véase* el párr. 36 de la sentencia). En el Asunto C-70/10, *Scarlet Extended SA v. SABAM* (2010), el TJUE sostuvo que un sistema de filtrado propuesto por los titulares de derechos con el fin de combatir la violación de los derechos de autor es ilegal, pues, le requeriría a los proveedores de servicios de Internet involucrarse en una "vigilancia preventiva" de las comunicaciones de los clientes en tiempo real y violaría el artículo 15(1) de la Directiva 2000/31, y probablemente rebasaría los derechos a la protección de datos y a la libertad de expresión de los artículos 8 y 11 de la Carta de los Derechos fundamentales de la UE.

45 *Véase* los artículos 8-11 de la CEDH, los artículo 12, 17, 18, 19, 21, y 22 del PIDCP, y los artículos 11, 12, 13, 15, y 16 de la CIDH.

46 Esto se nota especialmente en relación con el derecho a la intimidad. Por ejemplo, el artículo 8 del CEDH se refiere al derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia, mientras que el artículo 7 de la Carta de la UE se refiere al derecho al respeto de la vida privada y familiar, el domicilio y de las *comunicaciones*. Para un análisis más detallado del derecho a la intimidad en el PIDCP y otros instrumentos nacionales y regionales, *véase* el Relator Especial de las Naciones Unidas para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, A/HRC/13/37, 28 de diciembre 2009, párr. 11. Disponible en **http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf**.

47 *Véase* Relator Especial de las Naciones Unidas para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha

contra el Terrorismo, *Ibíd*., párrs. 16-18; *véase también* el Relator Especial de Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, A/HRC/23/40, 17 de abril de 2013, párrs. 28-29.

48 *Véase* la nota 45, *supra*. Otros artículos en los tratados de derechos humanos se refieren a la "ley", "legalidad" o "legal", como el artículo 5 del CEDH (protección frente a la detención y el encarcelamiento arbitrarios) y el artículo 7 del CEDH (no hay pena sin ley).

49 Comité de Derechos Humanos de la Naciones Unidas, Observación General No. 16 (1988), en *Instrumentos de Derechos Humanos, Volumen I, Recopilación de las Observaciones Generales y Recomendaciones Generales adoptadas por órganos Creados en virtud de Tratados de Derechos Humanos*, HRI/GEN/1/Rev.9 (Vol. I) 2008, pp. 191-193, párr. 4. *Véase también* Comité de Derechos Humanos de los Naciones Unidas, *Toonen v Australia*, Comunicación N º 488/1992, párr. 8.3, U.N.Doc CCPR/C/50/D/488/1992 (1994), y *Van Hulst v Países Bajos*, Comunicación N º 903/1999, párr. 7.6, U.N.Doc. CCPR/C/82/D/903/1999 (2004). En ambas comunicaciones, el Comité señaló que la razonabilidad también exige proporcionalidad. De manera más general, *véase* ACLU Privacy Rights In the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights, marzo de 2014. Disponible en **https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf**.

50 *Véase* Comité de Derechos Humanos de las Naciones Unidas, Comentario General no. 34 sobre libertad de opinión y expresión (artículo 19 de PIDCP). Disponible en **http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf**.

51 Sentencia en *Sunday Times v. Reino Unido*, no. 6538/74; 26 de abril de 1979, párr. 49.

52 En relación con el artículo 17 del PIDCP, *véase* las referencias en la nota 46, *supra*. El Tribunal Europeo de Derechos Humanos aplicó los principios desarrollados bajo el artículo 10 del CEDH (derecho a la libertad de expresión) en *Sunday Times* en el caso de *Silver y otros v. Reino Unido*, nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 de marzo de 1983, párrs. 85-86, en referencia al derecho a la intimidad de los presos bajo el artículo 8 del CEDH.

53 *Malone v. Reino Unido,* no. 8691/79, 2 de agosto de 1984, párr. 67.

54 *Ibíd*., párr. 68.

55 *Silver y otros v. Reino Unido*, *supra,* párr. 85-86 y *Malone v. Reino Unido, supra*, párr. 67.

56 *Malone v. Reino Unido*, párr. 67.

57 *Klass y otros v. Alemania*, no. 5029/71, 6 de septiembre de 1978, párrs. 42 y 49. En concreto, el Tribunal de Justicia declaró "El Tribunal, siendo conscientes del peligro que esa ley plantea al debilitar, e destruir la democracia alegando defenderla, afirma que los Estados contratantes no podrán, en nombre de la lucha contra el espionaje y el terrorismo, adoptar cualquiera medidas que consideren oportunas". *Véase también* la Oficina del Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Libertad de Expresión e Internet (OEA/Ser.L/V/II, CIDH/RELE/INF. 11/13, 31 de diciembre de 2013), párr. 150: "En lo que respecta al derecho a la libertad de expresión, la violación de la privacidad de las comunicaciones puede producir una restricción directa cuando—por ejemplo—el derecho no se puede ejercer de manera anónima como consecuencia de la actividad de vigilancia. Por otro lado, la mera existencia de este tipo de programas produce una limitación indirecta que genera un efecto inhibidor sobre el ejercicio de la libertad de expresión".

58 *Klass y otros v. Alemana*, *supra*, párr. 37.

59 *Véase Weber & Savaria v. Alemania*, no. 54934, 29 de junio de 2006, párr. 95.

60 *Véase*, en concreto, *Klass y otros v. Alemania*, *supra*, *Liberty y otros v. Reino Unido*, no. 58243/00, 1 de julio de 2008, y *Rotaru v. Rumania*, no. 28341/95,[GC], 4 de mayo de 2000, sobre la vigilancia llevada a cabo por las organismos de inteligencia. Para más detalles sobre la jurisprudencia de la CEDH en materia de vigilancia, *véase* Factsheet on the Protection of Personal Data. Disponible en **http://www.echr.coe.int/Documents/FS_Data_ENG.pdf**.

61 *Declaración conjunta sobre los programas de vigilancia y su impacto en la libertad de expresión*, emitido por el 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, junio de 2013, párrs. 8 y 9. Disponible en **http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1**

62 A/HRC/13/37, 28 de diciembre de 2009. Disponible en **http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf**.

63 *Véase*, por ejemplo, el artículo 19 del PIDCP (libertad de opinión y de expresión) se refiere al respeto de los derechos o la reputación de los demás, [o] para la protección de la seguridad nacional, el orden público o la salud o la moral públicas; el artículo 8 del CEDH (derecho a la intimidad) se refiere a "la seguridad nacional, la seguridad pública o el bienestar económico del país, para la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y la libertad de los demás"; el artículo 13 de la CIDH (libertad de expresión) se refiere al respeto de los derechos o la reputación de los demás, la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

64 *Véase* nota 46, *supra*.

65 *Véase*, por ejemplo, *Klass y otros, supra*, párr. 46.

66 Una rara excepción es *Uzun v. Alemania*, no. 35623/05, 2 de septiembre de 2010; *véase* también *Peck v. Reino Unido*, no. 44647/98, 28 de enero de 2003.

67 A/HRC/23/40, informe de 17 de abril de 2013, párr. 58. Disponible en **http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf**.

68 *Ibíd.*

69 *Véase*, por ejemplo, en Canadá: *R. v. Oakes*, 1 S.C.R. 103 (1986); *R. v. Big M Drug Mart Ltd*., 1 S.C.R. 295 (1985); en Estados Unidos: *Austin v. Michigan Chamber of Commerce*, 494 U.S. 652, 655 (1990); *Boos v. Barry*, 485 U.S. 312, 334 (1988) (pluralidad); *véase* también *Burson v. Freeman*, 504 U.S. 191, 198 (1992) (pluralidad); *Board of Airport Comm'rs v. Jews for Jesus*, *Inc*., 482 U.S. 569, 573 (1987); *Cornelius v. NAACP Legal Defense and Educ. Fund*, Inc., 473 U.S. 788, 800 (1985); *United States v. Grace*, 461 U.S. 171, 177 (1983); *Perry Educ. Ass'n v. Perry Local Educators' Ass'n*, 460 U.S. 37, 45 (1983).

70 Dictamen en la sentencia del Tribunal Constitucional de 27 de febrero de 2008 (1 BvR 370/07 y 1 BvR 595/07).

71 *Véase*, por ejemplo, al artículo 2(1) del PIDCP, los artículos 1.1 y 24 de CIDH, el artículo 14 del CEDH, el artículo 2 de la Convención Internacional para la Eliminación de Todas las Formas de Discriminación Racial, y al artículo 2 de la Convención para la Eliminación de Todas las Formas de Discriminación contra la Mujer. *Véase* también, por ejemplo, *Carson y otros v. Reino Unido,* 51 EHRR 13 (2010), en donde la Gran Sala del Tribunal Europeo de Derechos Humanos sostuvo que "cualquier otra condición social" según el artículo 14 del CEDH incluye "el país de residencia" (párr. 70-71).

72 Corte Interamericana de Derechos Humanos, Caso *Tristán Donoso v. Panamá*, Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 27 de enero de 2009. Serie C No. 193, párr. 56.

73 *Handyside v. Reino Unido*, no. 5493/72, 7 de diciembre de 1976, párrs. 48 y 49.

74 *Ibíd.*, párr. 48.

75 *Klass v. Germany*, párr. 42.

76 Observación General no. 27, 1999, CCPR/C/21/Rev.1/Add.9, reproducido en *Instrumentos de Derechos Humanos, Tomo I, Recopilación de las Observaciones Generales y Recomendaciones Generales adoptadas por órganos de Tratados de*

Derechos Humanos, HRI/GEN/1 / Rev. 9 (Vol. I) 2008, pp. 223-227, párrs. 11-16.

77 *Véase* Comentario General no. 34, *supra*, nota 20, párr. 34.

78 *Véase* la referencia en la nota 46, *supra.*

79 *Véase* Comentario General no. 34. *Ibíd*.

80 Tribunal Interamericana de Derechos Humanos, *Caso de Fontevecchia y D'Amico v. Argentina*, Fondo, Reparaciones y Costas Costs. Sentencia del 29 de noviembre de 2011. Series C No. 238, párr. 53.

81 *S y Marper v. Reino Unido,* 48 EHRR 50 (2009), párr. 118. El gobierno del Reino Unido admitió que la retención de datos de ADN "no fue garantizada por ningún grado de sospecha de participación de los demandantes en un delito o la propensión a la delincuencia, ni dirigida a los registros de retención en relación con presuntos delitos investigados en el pasado" (párr. 94).

82 *Gillan y Quinton v. Reino Unido,* 50 EHRR 45 (2010), párrs. 86-87.

83 Asuntos acumulados C-293/12 y C-594/12, 8 de abril de 2014.

84 *Ibíd*., párr. 56.

85 *Ibíd*., párr. 58.

86 Privacy International, Electronic Frontier Foundation, Access, APC, ARTICLE 19, Human Rights Watch et al., *OHCHR consultation in connection with General Assembly Resolution 68/167 "The right to privacy in the digital age,"* 1 de abril de 2014. Disponible en **https://www.eff.org/files/2014/04/17/ngo_submission_final_31.03.14.pdf**.

87 *Véase*, por ejemplo, *Weber y Savaria v. Alemania, supra*, párr. 95, en el que el Tribunal identifica varias "salvaguardas mínimas que deben establecerse en leyes estatutarias para evitar el 'abuso de poder'" (párr. 95).

88 2 EHRR 214 (1979-1980), párr. 55.

89 *Klass v. Germany, supra*, párr. 56.

90 *Kopp v. Suiza,* 27 EHRR 91 (1999), párr. 74.

91 *Véase* **http://news.mt.co.kr/mtview.php?no=2014041611218282360** (Corea).

92 *Véase* Decisión de la Tribunal 2010 Hunma 47, 252 (consolidada), anunciada el 28 de agosto de 2012, y decisiones subsecuentes del Alto Tribunal coreano en octubre de 2012 (Alto Tribunal de Seúl, 2011Na19012, Juez Presidente Kim Sang-Jun) que sostuvo la responsabilidad de un importante portal por revelar a la policía la identidad de un blogger sin una orden judicial.

93 Comité de Derechos Humanos de las Naciones Unidas, Observaciones finales sobre el Cuarto Informe de EE.UU., 27 de marzo de 2014. Disponible en **http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf**, párr. 22.

94 Para un análisis del potencial impacto de estas prácticas, *véase* K.S. Bankston, "Only the DOJ Knows: The Secret Law of Electronic Surveillance", (2007) 41 Univ. S.F. L. Rev. 589. Disponible en **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2009442**.

95 *Véase* Eric Metcalfe, *Secret Evidence*, JUSTICE, junio de 2009, p. 177. Disponible en **http://www.justice.org.uk/data/files/resources/33/Secret-Evidence-10-June-2009.pdf**.

96 *Véase* Ibíd., p. 173 para la discusión del modelo canadiense del Comité de Revisión de Inteligencia de Seguridad y la p. 231 para propuestas que introducen defensas al interés público. Cada vez es más común en los tribunales del Reino Unido asignar un defensor de inmunidad del interés público: *véase*, por ejemplo, *CM (Zimbabue) v. Secretario de Estado del Ministerio del Interior,* EWCA Civ 1303 *Interior* (2013). *Véase* el informe más reciente del Congressional Research Service, *Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate,* 21 de marzo de 2014. Disponible en **http://www.fas.org/sgp/crs/intel/R43451.pdf**.

97 *Véase*, por ejemplo, la discusión de la necesidad de una autorización judicial previa en el contexto del registro de computadores en la sentencia de la Corte Suprema canadiense en *R. v. Vu*, 2013 SCC 60. Disponible en **http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13327/index.do**.

98 Para más detalles *véase* la sección de Notificación del Usuario.

99 *Véase* Jennifer Stisa Granick & Christopher Jon Sprigman, *NSA, DEA, IRS Lie About Fact That Americans Are Routinely Spied On By Our Government: Time For A Special Prosecutor*, 14 de agosto de 2013. Disponible en **http://www.forbes.com/sites/jennifergranick/2013/08/14/nsa-dea-irs-lie-about-fact-that-americans-are-routinely-spied-on-by-our-government-time-for-a-special-prosecutor-2/**.

100 EL derecho a juicio justo está garantizado en el artículo 10 de la DUDH, el artículo 6 de la CEDH, el artículo 8 del CIDH y el artículo 14 del PIDCP. El derecho a un recurso efectivo está protegido en el artículo 8 de la DUDH, el artículo 15 del CIDH, el artículo 13 de la CEDH y el artículo 2.3 del PIDCP. En la Carta de la Unión Europea, ambos derechos están protegidos en el artículo 47.

101 *Véase*, por ejemplo, *Ashby v. White* 92 ER 126 (1703) por Lord Holt CJ: "es vano imaginar un derecho sin recurso, la ausencia de un derecho y la ausencia de un remedio son recíprocas".

102 *Véase*, en concreto, el artículo 8 de la *Convención para la Protección de las Personas relativa al Tratamiento Automatizado de Datos de Carácter Personal* (Convenio No. 108) del Consejo Europeo de 1981 y de los artículos 10, 11 y 12, así como los artículos 18 y 19 de la *Directiva comunitaria sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* de 1995 (Directiva 95/46/CE). Para una discusión extensa, vinculada a la evolución tecnológica, *véase* Douwe Korff *Working Paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments*, preparados por Douwe Korff y Ian Brown, *et al., Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, estudio comisionado por la Comisión Europea, 2010. Disponible en **http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf**.

103 *Véase Klass v. Germany,* 2 EHRR 214 (1979-80), párr. 58: "En la opinión del Tribunal, ha de examinarse si es aún posible en la práctica requerir la notificación posterior en todos los casos. La actividad o peligro contra el que se dirige una serie particular de medidas de vigilancia puede durar años, incluso décadas, después de la suspensión de esas medidas. La notificación posterior a cada persona afectada por una medida de suspensión bien podría poner en peligro el objetivo a largo plazo que originalmente llevó a la vigilancia. Por otra parte...tal notificación puede servir para revelar los métodos y campos de trabajo de operación de los servicios de inteligencia e incluso, posiblemente, a la identificación de sus agentes. En opinión del Tribunal, en la medida en que la 'interferencia' que resulta de la legislación impugnada, en principio, se justifica en virtud del Art. 8(2)...el hecho de no informar a la persona una vez ha cesado la vigilancia no puede ser en sí mismo incompatible con esta disposición, puesto que es este mismo hecho lo que garantiza la eficacia de la 'interferencia'."

104 *Association for European Integration and Human Rights and Ekimdzhievv. Bulgaria*, 62540/00, 28 de junio de 2007, párr. 90. *Véase* también *Weber y Savaria v. Alemania,* donde el Tribunal reitera que la notificación puede constituir una importante salvaguarda, no siendo del todo necesaria.

105 *Véase Freedom from Suspicion: Surveillance Reform for a Digital Age* (JUSTICE, octubre de 2011).

106 ***Véase Código Penal***, R.S.C., 1985, c. C-46, Sección VI. La Sección VI ha operado efectivamente por muchas tiempo, demostrando que los requisitos de notificación individual son prácticamente viables. Además, la Corte Suprema de Canadá recientemente ha dado pasos para reconocer que las obligaciones de la notificación individual son un imperativo constitucional bajo la sección 8 de la ***Carta de Derechos y Libertades***, que garantiza el derecho a estar protegidos de registros e incautaciones arbitrarias: ***R. v. Tse***, 2012 SCC 16, párr. 11 (el requisito constitucional de la notificación individual para escuchas telefónicas en donde no hay una autorización judicial previa por razón de

circunstancias apremiantes); ***R. v TELUS Communications Co.***, 2013 SCC 16, párr. 30 ("una disposición de notificación era necesaria para cumplir los estándares constitucionales mínimos de la protección de la sección 8 contra el registro e incautación arbitrarios, pero en obiter"); ***R. v. Chehil***, 2013 SCC 49, párr. 58 ("la notificación con posterioridad al registro que no está sujetq a una autorización judicial previa es una importante salvaguardia contra el abuso de estos poderes", en referencia a la detención de drogas por perros olfateando la maleta de alguien). La sección de Estados Unidos 50 USC 2518 (8)(d) requiere notificación por escuchas telefónicas "dentro de un plazo razonable, pero no más tarde de noventa días después de la presentación de una solicitud de una orden de aprobación." Sin embargo, ninguno de estos requisitos se han aplicado a la vigilancia llevada a cabo por los organismos de inteligencia extranjeros.

107 Por ejemplo, la legislación coreana, que permite el retraso de la notificación del usuario tras la aprobación del Fiscal General Regional, violaría los Principios. Ley de protección del secreto de las comunicaciones, Artículo 9-2 (5).

108 *Véase* ARTICLE 19, *The Public's Right to Know: Principles on Freedom of Information Legislation,* junio de 1999.

109 *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.**

110 *Klass*, párr. 42. *Véase* también el párr. 49: "El Tribunal, siendo conscientes del peligro que esa ley plantea al debilitar, e incluso destruir la democracia alegando defenderla, afirma que los Estados contratantes no podrán, en nombre de la lucha contra el espionaje y el terrorismo, adoptar cualquiera medidas que consideren oportunas".

111 *Malone v. United Kingdom*, párr. 67.

112 *Huvig v.* France, 12 EHRR 528 (1990), párrs. 29-35.

113 Cindy Cohn, Mark Jaycox, *NSA Spying: The Three Pillars of Government Trust Have Fallen*, 15 de agosto 2013. Disponible en **https://www.eff.org/deeplinks/2013/08/nsa-spying-three-pillars-government-trust-have-fallen**.

114 *Véase* también, 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/opinion-recommendation/files/2014/wp215_en.pdf**.

115 *Véase,* en concreto, los Principios 2 y 3 del Principio del Derecho a Saber (nota 109, *supra*).

116 *Véase* Kurt Opsahl, Crucial Unanswered Questions about the NSA's BULLRUN Program. Disponible en **https://www.eff.org/deeplinks/2013/09/crucial-unanswered-questions-about-nsa-bullrun-program**.

117 Informe del Relator Especial para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión (A.HRC/23/40, 17 de abril de 2013), párr. 79.

118 Informe del Relator Especial para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Frank La Rue, 16 de mayo de 2011, A/HRC/17/27, párr. 84.

119 CCPR/C/USA/CO/4, 23 de abril de 2014, párr. 22.

120 ***Véase***, por ejemplo, el artículo 14(2) del PIDCP y el artículo 6(2). En ***S y Marper***, ***supra***, la Gran Sala señaló que si bien "es cierto que la retención de los datos privados de los demandantes no se puede equiparar con las expresiones de sospechoso", no obstante, la presunción era pertinente para evaluar la proporcionalidad, puesto que la percepción de las personas cuyos datos eran conservados de "que no eran tratados como inocente suele ir acompañada por el hecho de que los datos se conservan indefinidamente en la misma forma que los datos de las personas condenadas, mientras que se requiere la destrucción de los datos de aquellos que no han sido sospechosos" (párr. 122).

121 Para un análisis académico más profundo y referencias más extensas de la jurisprudencia del Comité de Derechos Humanos y otras fuentes, *véase* Martin Scheinin & Mathias Vermeulen, "Unilateral Exceptions to International Law: Systematic legal Analysis and Critique of Doctrines that seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism," sección 3.7 en *Denial of Extraterritorial Effect of Human Rights (Treaties)*. Disponible en **http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf**.

122 Ian Brownlie, *Principles of Public International Law*, 6th ed., 2006, p. 306. La expresión clásica del principio puede verse en el laudo del árbitro único en el caso *Isla de Palmas*, Max Huber: "*La soberanía en las relaciones entre los Estados significa independencia. Independencia con respecto a una parte del mundo es el derecho a ejercer las funciones de un Estado, con exclusión de cualquier otro. El desarrollo de la organización nacional de los Estados en los últimos siglos y, como corolario, el desarrollo del derecho internacional han establecido este principio de la competencia exclusiva del Estado en lo que respecta a su propio territorio, de forma que es el punto de partido para la solución de la mayoría de las preguntas respecto a las relaciones internacionales*". *Island of Palmas Case* (*Países Bajos/Estados Unidos de América*), Laudo del 4 de abril de 1928, UNRIAA, vol. II (1928), pp. 829-871, 838. Disponible en **http://legal.un.org/riaa/cases/vol_II/829-871.pdf**. *Véase* también la *sentencia Lotus* de la Corte Permanente de Justicia Internacional (la precursora de

la Corte Internacional de Justicia), 7 de septiembre de 1927, pp. 18-19. Disponible en **http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.**

123 Informe de la Comisión de Derecho Internacional de 2006, Anexo E (nota 83, *supra*), párr. 22, p. 526, [Énfasis añadido].

124 Sobre la conferencia, ***véase*** Consejo de Europa, Conferencia Octopus—Cooperación contra la Ciberdelicuencia, 4-6 de diciembre de 2013. Disponible en **http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp.** En el momento en que se redactó este documento (diciembre de 2013), las actas y conclusiones no había sido publicado aún, pero en la sesión de clausura fue ampliamente aceptada la necesidad de un nuevo protocolo, a pesar de que la naturaleza de este instrumento aún no estaba muy claro, pues las opciones de "consentimiento" recogidas en un documento de 2013 no eran suficientes (en el mismo se hace referencia al consentimiento de los datos objeto/sospechosos, acordándose que no puede suponerse que se han dado de forma voluntaria; y para otorgar su consentimiento a otros con "autoridad legal" para revelar los datos [léase: proveedores de servicios de Internet y comunicaciones electrónicas], acordándose que ellos no estaban en condiciones de tomar la decisión pertinente sobre la divulgación). Por tanto, el tema se abordará tras un análisis más profundo.

125 *Véase*, por ejemplo, la sentencia de la Convención Europea de Derechos Humanos en *CAS y CS v. Rumania*, no. 26692/05, 20 de marzo de 2012, párr. 71: "las obligaciones positivas del Estado son inherentes al derecho al respeto efectivo de la vida privada bajo el artículo 8; estas obligaciones pueden implicar la adopción de medidas, incluso en la esfera de las relaciones entre las personas".

126 *Véase*, por ejemplo, artículo 2(3)(a) del PIDCP, el artículo 13 del CEDH.

127 *Véase* también el artículo 10 del CEDH. En el caso seminal de *Guja v Moldavia* (no. 14277/04, 12 de febrero de 2008), la Gran Sala del TEDH sostuvo que la señalización por un funcionario o un empleado del sector público de la conducta ilegal o delito en el lugar de trabajo debe, en ciertas circunstancias, gozar de protección. El Tribunal llegó a sostener que en el examen de cualquier injerencia en el derecho a la libertad de expresión de los denunciantes, deberá prestarse especial consideración al interés público involucrado en la información revelada (párr. 74) y el motivo detrás de las acciones del empleado denunciante (párr. 77).

128 *Véase*, por ejemplo, Comité de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial para la Promoción y Protección del Derecho a la Opinión y Expresión, Abid Hussain, presentada de conformidad con la resolución 1999/36 E/CN.4/2000/63, 18 de enero de 2000; *véase* también la 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.

129 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.

130 En particular, los Principios de Johannesburgo establecen que nadie puede ser castigado por razones de seguridad nacional por divulgar información si: (i) la divulgación efectivamente no causa daño y no es probable que cause daño a un interés legítimo de seguridad nacional, o (ii) el interés público en conocer la información es mayor que el daño causado por la divulgación.

131 Los Principios de Tschwane establecen que la ley debe proteger de represalias a quienes revelen actos ilegales si, entre otras cosas, el denunciante "razonablemente creía que había, de hacer la divulgación interna y/o a un órgano de supervisión independiente, un riesgo significativo que habría dado lugar a la destrucción u ocultamiento de la prueba, la interferencia con un testigo o represalia contra la persona o un tercero" y "razonablemente creía que el interés público en disponer de la información revelada supera el daño al interés público que resultaría de la divulgación".

132 La legislación de los EE.UU. es particularmente débil en este sentido, *véase* Trevor Timm, *If Snowden Returned to US for Trial, All Whistleblower Evidence Would Likely Be Inadmissible*, 23 de diciembre de 2013. Disponible en **https://huffingtonpost.com/trevor-timm/if-snowden-returned-to-us_b_4495027.html**. Además, si bien la Intelligence Community Whistleblower Protection Act de 1998, establece un procedimiento para la elaboración de informes internos dentro de las agencias y a través de la Inspección General de los comités de inteligencia del Congreso, no proporciona solución alguna contra las represalias que se producen como consecuencia de ello.

133 *Véase Silverthorne Lumber Co v. United States*, 251 U.S. 385 (1920).

134 *Véase*, por ejemplo, las sentencias del Tribunal Europeo de Derechos en *Schenk v. Suiza*, 13 EHRR 242 (1988) y *Chinoy v. Reino Unido*, no. 15199/89, 4 de septiembre de 1991.

135 *Véase*, por ejemplo, la sentencia del Tribunal Europeo de Derechos Humanos en *Khan* v. Reino Unido, 31 EHRR 45 (2000), párr. 34: "La pregunta que debe responderse es si el proceso en su conjunto, incluida la forma en que se obtuvo la prueba, fue justo. Esto implica un examen de la 'ilegalidad' en cuestión y, con respecto a la violación de otro derecho de la Convención, la naturaleza de la violación encontrada".

necessaryandproportionate.org/LegalAnalysis