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, Asociación por los Derechos Civiles, 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.

Para máss información, puedes visitar la siguiente página.

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.

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 ac-

erca 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 so-

bre 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. 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.

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 gubernamen-

tal. 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.