Asociación de Internautas

De le defensa del derecho fundamental a la privacidad a la vigilancia masiva

De le defensa del derecho fundamental a la privacidad a la vigilancia masiva

A medida que avanzan las tecnologías que facilitan la vigilancia estatal de las comunicaciones, los Estados están fallando en garantizar que las leyes y regulaciones relacionadas con la vigilancia de las comunicaciones estén en consonacia con el derecho internacional de los derechos humanos y protejan adecuadamente los derechos a la intimidad y a la libertad de expresión. Este documento intenta explicar 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, en los que ha participado la Asociación de Internautas, con la industria y expertos internacionales en legislación sobre vigilancia de las comunicaciones, políticas públicas y tecnología.

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.[s.[1]

Las actividades que restringen el derecho a la intimidad, incluida la vigilancia de las comunicaciones, únicamente pueden justificarse cuando están prescritas por ley, son necesarias para alcanzar un objetivo legítimo y son proporcionales al fin 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 estatal de las comunicaciones. 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, o ?metadatos de comunicaciones? ? 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 la vigilancia 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 capacidades estatales de vigilancia de comunicaciones, la habilidad del Estado para combinar y organizar la información obtenida mediante distintas técnicas 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 comnunicaciones aumenta drásticamente, sin controles adecuados.[4]

Acceder a los metadatos de las comunicaciones y analizarlos permite crear perfiles de la vida de las personas, condiciones médicas, orientaciones políticas y religiosas, asociaciones, interacciones e intereses, revelando tanto o más detalles que el que podría apreciarse a partir del contenido de las comunicaciones. [5] A pesar del enorme potencial de intrusión en la vida de una persona y del efecto amedrentador sobre las asociaciones políticas y de otro tipo, los instrumentos legislativos y de políticas públicas a menudo otorgan a los metadatos de comunicaciones un menor nivel de protección, y no imponen restricciones suficientes sobre cómo pueden ser posteriormente utilizados por los organismos del Estado, incluyendo la forma en que son minados, compartidos y conservados.

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, sea ésta el cumplimiento de la ley, la seguridad nacional o cualquier otro propósito normativo. 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, incluidas las personas jurídicas.[6]

El sector privado asume la misma responsabilidad de respetar los derechos humanos, en especial teniendo en cuenta el papel fundamental que desempeña en el diseño, desarrollo y difusión de las tecnologías, activación y suministro de las comunicaciones, y ? cuando se le requiere ? en la cooperación con las actividades de vigilancia estatal. Sin embargo, el alcance de los presentes Principios se limita a las obligaciones del Estado.

Cambio de tecnología y definiciones

«Vigilancia de 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.

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 que incluye, refleja, surge de o es sobre las comunicaciones de una persona y que no está disponible ni es de fácil acceso para el público general, debería ser considerada como "información protegida", y por lo tanto se le debería dar la más alta 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. La 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 requierenque 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 Principios

Legalidad: Cualquier limitación al derecho a la privacidad 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 nivel 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: Las leyes que permiten la vigilancia de las comunicaciones por el Estado deben limitar dicha vigilancia 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 a la privacidad y la libertad de opinión y de expresión, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la vigilancia de las comunicaciones deben tomarse sopesando el beneficio que se persigue contra el daño que se causaría a los derechos de las personas y contra otros intereses en conflicto, y debería incluir un examen de la sensibilidad de la información y de la gravedad de la infracción al derecho a la privacidad.

En concreto, esto requiere que si un Estado busca acceder o usar información protegida obtenida a través de vigilancia de las comunicaciones en el marco de una investigación penal, debe establecer ante una autoridad judicial competente, independiente e imparcial que:

1. existe un alto grado de probabilidad de que un grave delito ha sido cometido o será cometido;

2. la evidencia sobre tal delito sería obtenida al acceder a la información protegida que se busca;

3. otras técnicas de investigación que son menos invasivas y están disponibles ya han sido agotadas;

4. la información a la que se accede se limitará a la razonablemente relevante para el presunto delito y cualquier exceso en la información recopilada será destruido o devuelto sin demora, y

5. solo tendrá acceso a la información la autoridad especificada y se utilizará solo para el propósito para el cual se le dio autorización.

Si el Estado busca el acceso a la información protegida a través de la vigilancia de las comunicaciones para un propósito que no pone a una persona en riesgo de persecución penal, investigación, discriminación o violación de derechos humanos, el Estado debe establecer ante una autoridad independiente, imparcial y competente que:

1. otras técnicas de investigación que son menos invasivas y están disponibles han sido consideradas;
2. la información a la que se accede se limitará a la que sea razonable y relevante y cualquier exceso de información recopilada será destruido o devuelto a la persona afectada sin demora, y
3. a la información solo tendrá acceso la autoridad especificada y se utilizará solo para el propósito para el cual se le dio autorización.

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 de las autoridades encargadas de la vigilancia de las comunicaciones, (2) ser experta ??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: Las personas deben ser notificadas de una decisión que autoriza la vigilancia de las comunicaciones con el tiempo e información suficientes para permitirles recurrir la decisión, 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. La persona afectada es notificada tan pronto como el riesgo desaparece o dentro de un período de tiempo razonable y factible, según lo que ocurra primero, y en todo caso en el momento en que la vigilancia de las comunicaciones se ha completado.

La obligación de notificar recae en el Estado, pero en el caso de que el Estado no haya dado aviso, los proveedores de servicios de comunicaciones están en libertad de notificar a las personas de la vigilancia de las comunicaciones, sea de manera voluntaria o previa solicitud.

Transparencia: Los Estados deben ser transparentes sobre el uso y alcance de las técnicas y poderes de la vigilancia de las comunicaciones. Deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, 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 deben permitir que los proveedores de servicios publiquen los procedimientos que ellos aplican cuando se trata de la vigilancia estatal de las comunicaciones, se adhieran a esos procedimientos y publiquen los registros de vigilancia de las comunicaciones del Estado.

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 publicar informes periódicos y otra información relevante sobre la vigilancia de las comunicaciones. Además de cualquier supervisión ya proporcionada a través de otra rama del gobierno, deben establecerse mecanismos de supervisión independientes.

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 terminus 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 estatal. 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 como condición previa para la prestación de servicios.[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. 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 norma 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 recíprova y otros acuerdos deben estar claramente documentados, a disposición del público y sujetos a las garantías de equidad procesal.

Garantías contra el acceso ilegítimo: Los Estados deben promulgar leyes que penalicen la vigilancia ilegal de las comunicaciones por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los denunciantes (?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 debe ser destruido o devuelto a la persona.

[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 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.

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&boar

[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]"People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[8] "People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[9]"Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups ? and not just one such fact about a person, but all such facts." U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.)p. 562; U.S. v. Jones, 565 U.S. __, (2012), Alito, J., concurring. "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past?In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls

within the scope of 'private life' for the purposes of Article 8(1) of the Convention." (Rotaru v. Romania, [2000] ECHR 28341/95, paras. 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 Unid