RELATORÍA ESPECIAL PARA LA LIBERTAD DE EXPRESIÓN

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos tiene el honor de dirigirse a la Misión Permanente de la República del Perú ante la Organización de los Estados Americanos, con el objeto de transmitirle una solicitud de información dirigida a su Ministerio de Relaciones Exteriores.

La Relatoría Especial para la Libertad de Expresión aprovecha la oportunidad para expresar a la Misión Permanente de la República del Perú el testimonio de su más alta y distinguida consideración.

28 de Agosto de 2015

RELATORÍA ESPECIAL PARA LA LIBERTAD DE EXPRESIÓN

Washington, D.C., 28 de agosto de 2015

REF: Decreto Legislativo No. 1182 "Que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado".
Solicitud de información conforme al artículo 41 de la CADH

Excelentísima Sra. Ana María Liliana Sánchez Vargas de Ríos,

Tengo el honor de dirigirme a usted en mi carácter de Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), conforme a las facultades establecidas en el artículo 41 de la Convención Americana sobre Derechos Humanos, con el objetivo de solicitar información a propósito del Decreto Legislativo No. 1182 de referencia y formular algunas recomendaciones a la luz de la Convención Americana sobre Derechos Humanos.

La Relatoría Especial recibió información sobre la aprobación el pasado 26 de julio de 2015 del Decreto Legislativo No. 1182, el cual tiene por objeto "regular el acceso de la unidad especializada de la Policía Nacional del Perú, en casos de flagrancia delictiva, a la localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar". Asimismo, el Decreto Legislativo establece la obligación de conservación de datos de tráfico derivados de las telecomunicaciones por un periodo de tres años y su acceso por parte de las autoridades estatales en el marco de la investigación de delitos. El Decreto Legislativo ha sido cuestionado por diversas organizaciones de la sociedad civil en el Perú, quienes afirmaron que la normativa no había sido objeto de discusión pública en el Congreso Nacional, por lo que han solicitado su revisión.

El Decreto Legislativo dispone que "la unidad a cargo de la investigación policial solicita a la unidad especializada el acceso inmediato a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, siempre que concurran los siguientes presupuestos: a. Cuando se trate de flagrante delito, de conformidad con lo dispuesto en el artículo 259 del Decreto Legislativo Nº 957, Código Procesal Penal. b. Cuando el delito investigado sea sancionado con pena superior a los cuatro años de privación de libertad. c. El acceso a los datos constituya un medio necesario para la investigación". (Art. 3)

"Una vez verificados los supuestos del artículo precedente, pone en conocimiento del Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la Policía Nacional del Perú para efectos de la localización o geolocalización". Hecha la solicitud, "los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata". (Art. 4)

Excelentísima señora
Ana María Liliana Sánchez Vargas de Ríos
Ministra de Relaciones Exteriores
República del Parú

De conformidad con el Decreto Legislativo, "la unidad a cargo de la investigación policial, dentro de las 24 horas de comunicado el hecho al Fiscal correspondiente, le remitirá un informe que sustente el requerimiento para su convalidación judicial". Por su parte, "el Fiscal dentro de las veinticuatro (24) horas de recibido el informe, solicita al Juez la convalidación de la medida. El juez competente resolverá mediante trámite reservado y de manera inmediata, teniendo a la vista los recaudos del requerimiento fiscal, en un plazo no mayor de 24 horas. La denegación del requerimiento deja sin efecto la medida y podrá ser apelada por el Fiscal. El recurso ante el juez superior se resolverá en el mismo plazo y sin trámite alguno. El juez que convalida la medida establecerá un plazo que no excederá de sesenta (60) días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal". (Art. 5)

Asimismo, la disposición complementaria final segunda del Decreto Legislativo No. 1182, la cual dispone que: "Los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas relacionadas con estos servicios deben conservar los datos derivados de las telecomunicaciones durante los primeros doce (12) meses en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real. Concluido el referido periodo, deberán conservar dichos datos por veinticuatro (24) meses adicionales, en un sistema de almacenamiento electrónico. La entrega de datos almacenados por un periodo no mayor a doce meses, se realiza en línea y en tiempo real después de recibida la autorización judicial. Para el caso de los datos almacenados por un periodo mayor a doce meses, se hará entrega dentro de los siete (7) días siguientes a la autorización judicial, bajo responsabilidad".

En virtud de lo anterior y dada la importancia del objeto de regulación, la Relatoría Especial se permite poner de presente algunos aspectos del derecho internacional de los derechos humanos que resultaría relevante que el Ilustre Estado de Perú tuviese en cuenta en el actual debate sobre la normativa. En particular, esta comunicación pone de presente el reciente desarrollo del marco jurídico internacional en cuanto a los derechos a la libertad de pensamiento y expresión y a la intimidad en la era digital.

1. La libertad de pensamiento y expresión en el entorno digital y su relación con el derecho a la privacidad

En su informe Libertad de Expresión e Internet, la Relatoría Especial destacó la importancia y el carácter transformador que tiene Internet para el ejercicio del derecho a la libertad de expresión y la promoción del intercambio en tiempo real de información y opiniones en amplios y diversos sectores de la población. Asimismo, subrayó el potencial de Internet para promover el pleno goce y ejercicio de otros derechos humanos, así como para facilitar el acceso a bienes y servicios[1].

Al tiempo que Internet ha creado oportunidades sin precedentes para la libre expresión, comunicación, búsqueda, posesión e intercambio de información, ha facilitado la recolección y desarrollo de grandes cantidades de datos acerca de las personas. En la era digital, la tecnología disponible para captar y monitorear comunicaciones y actividades privadas ha cambiado vertiginosamente, aumentando los desafíos para la protección de la privacidad de las personas, con un impacto cierto en el ejercicio del derecho a la libertad de pensamiento y expresión[2].

Al respecto, como ya ha sido expuesto por esta oficina[3], el derecho a la privacidad protege al menos cuatro bienes jurídicos, que tienen una relación estrecha con el ejercicio de la libertad de pensamiento y

[1] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013.

[2] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013; Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). 1 de junio de 2011. *Declaración conjunta sobre libertad de expresión e Internet*.

[3] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013, párr. 131.

expresión. En primer lugar, el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas. En segundo lugar, el derecho a gobernarse, en ese espacio de soledad, por reglas propias definidas de manera autónoma según el proyecto individual de vida de cada uno. En tercer lugar, el derecho a la vida privada protege el secreto de todos los datos que se produzcan en ese espacio reservado, es decir, prohíbe la divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona. Y, finalmente, la protección de la vida privada protege el derecho a la propia imagen, es decir, el derecho a que la imagen no sea utilizada sin el consentimiento del titular[4].

Esta oficina ha destacado que en virtud de esta relación estrecha entre libertad de expresión y privacidad, los Estados deben evitar la implementación de cualquier medida que restrinja, de manera arbitraria o abusiva, la privacidad de los individuos (artículo 11 de la Convención Americana[5]), entendida en sentido amplio como todo espacio de intimidad y anonimato, libre de amedrentamiento y de represalias, y necesario para que un individuo pueda formarse libremente una opinión y expresar sus ideas así como buscar y recibir información, sin ser forzado a identificarse o a revelar sus creencias y convicciones o las fuentes que consulta[6].

Bajo esta premisa, la Relatoría Especial ha recomendado a los Estados de la región que cualquier tipo de regulación que pueda afectar de una u otra manera el acceso y uso de Internet - no solo de manera directa sino también a través de los particulares que influyen y determinan su desarrollo - debe tomar en cuenta las características originales y diferenciales de Internet, como medio privilegiado para el ejercicio cada vez más democrático, abierto, plural y expansivo de la libertad de expresión y como un espacio para el desenvolvimiento de la intimidad sin precedentes[7].

2. La vigilancia de las comunicaciones en línea

La Relatoría Especial ha reconocido que en algunas oportunidades resulta legítimo el uso excepcional de programas o sistemas de vigilancia en las comunicaciones privadas establecidos en la ley, cuando quiera que sean necesarios, por ejemplo, para el cumplimiento de fines imperativos como la prevención del delito.

En efecto, en su informe sobre Seguridad Ciudadana y Derechos Humanos, la CIDH advirtió que la inseguridad generada por la criminalidad y la violencia en las Américas constituye un grave problema donde está en juego la vigencia de los derechos humanos, genera alarmas para la gobernabilidad democrática y la vigencia del Estado de Derecho[8]. A partir de su obligación de garantizar a las personas el ejercicio libre de sus derechos, los Estados han adoptado medidas de distinta índole para prevenir y contrarrestar la violencia e inseguridad, y en especial aquella que surge del crimen organizado, incluidas la formulación de leyes y procedimientos internos para prevenir, investigar, judicializar y sancionar la comisión de crímenes y actividades ilícitas.

Al tomar iniciativas de seguridad ciudadana, los Estados deben cumplir sus obligaciones internacionales, incluidas las asumidas dentro de los marcos del derecho internacional de los derechos

[4] CIDH. Informe No. 82/10. Caso No. 12.524. Fontevecchia y D'Amico. Argentina. 13 de julio de 2010. Párr. 91 y ss.

[5] El artículo 11 de la Convención Americana sobre Derechos Humanos establece que "[n]adie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación", y que "[t]oda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

[6] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. En igual sentido, Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40. 17 de abril de 2013. Párr. 47; Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27. 16 de mayo de 2011. Párr. 53, 82 y 84.

[7] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013.

[8] CIDH. Informe sobre Seguridad Ciudadana y Derechos Humanos. OEA/Ser.L/V/II. Doc. 57. 31 de diciembre de 2009.

humanos. En tal sentido, la CIDH ha subrayado sistemáticamente que el respeto irrestricto del pleno goce de los derechos humanos debe ser parte fundamental de cualquier estrategia en esta materia.

Como se dijo anteriormente, la protección de la seguridad ciudadana y la lucha contra el crimen organizado son fines legítimos que pueden justificar el uso excepcional de vigilancia en las comunicaciones privadas. No obstante, tal y como se indicó, los Estados deben garantizar que la captura y conservación de datos sobre las comunicaciones digitales estén "claramente autorizados por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados. La ley deberá atender a un objetivo legítimo y 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"[9].

En su Informe sobre Libertad de Expresión e Internet, la Relatoría Especial indicó que la interceptación y retención de datos sobre las comunicaciones privadas comporta tanto una limitación directa al derecho a la intimidad como una afectación del derecho a la libertad de pensamiento y expresión. Para que esta limitación pueda considerarse legítima, debe cumplir con una serie de condiciones impuestas de conformidad con los artículos 11, 13, 8 y 25 de la Convención Americana. Esto es: (1) consagración legal; (2) búsqueda de una finalidad imperativa; (3) necesidad, idoneidad y proporcionalidad de la medida para alcanzar la finalidad perseguida; (4) garantías judiciales; y (5) satisfacción del debido proceso.

Tal y como se expresó esta oficina, este tipo de medidas debe encontrarse establecida por medio de leyes en sentido formal y material, lo que significa que debe ser una ley fruto de la deliberación propia del órgano legislativo la que defina de manera precisa las causas y condiciones que habilitarían al Estado a interceptar las comunicaciones de las personas, a recoger datos de comunicación o "metadatos", o a someterlas a una vigilancia o seguimiento que invada esferas en las que tienen razonables expectativas de privacidad[10].

Como lo ha dicho en otras oportunidades, "serían incompatibles con la Convención Americana las restricciones sustantivas definidas en disposiciones administrativas o las regulaciones amplias o ambiguas que no generan certeza sobre el ámbito del derecho protegido y cuya interpretación puede dar lugar a decisiones arbitrarias que comprometan de forma ilegítima los derechos a la intimidad y a la libertad de expresión"[11].

Además de contar con base legal, la Relatoría Especial ha instado los Estados a evaluar la necesidad y proporcionalidad de toda afectación al ejercicio de derechos en Internet, ponderando el impacto que podría tener en la capacidad de este medio para garantizar y promover la libertad de expresión con respecto a los beneficios que la restricción reportaría para la protección de otros intereses. Para ello, es necesario tener en cuenta la disponibilidad de medidas menos restrictivas sobre los derechos involucrados.

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 sólo en las circunstancias más excepcionales definidas en la legislación. Cuando se invoquen causales más o menos abiertas como 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.

Asimismo, la Relatoría ha indicado que cualquier restricción a la libertad de expresión o a la privacidad en Internet como efecto de una medida estatal de seguridad debe respetar los requisitos procedimentales impuestos por el derecho interamericano. En efecto, el artículo 8 de la Convención

[9] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013.

[10] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. Párr. 153.

[11] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013.

Americana no limita su aplicación a recursos judiciales sino que debe entenderse como "el conjunto de requisitos que deben observarse en las instancias procesales a efecto de que las personas puedan defenderse adecuadamente ante cualquier tipo de acto emanado del Estado que pueda afectar sus derechos". En este sentido, la necesidad de que existan controles efectivos para asegurar que los programas de vigilancia de la información en línea sean diseñados e implementados teniendo en consideración todos los derechos en juego, incluyendo las garantías procesales. En virtud de los anterior, las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover. Con este fin, la autoridad judicial debe 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. Debe asimismo, contar con los recursos adecuados en el ejercicio de las funciones que se le asignen.

3. La Retención Obligatoria e Indiscriminada de Datos Electrónicos

Desde hace algunos años los países de la región han impulsado regulaciones que obligan a los servicios de telecomunicaciones y otros proveedores de servicios de Internet a capturar y conservar de manera indiscriminada los datos de registro – o metadatos- generados sobre las comunicaciones y actividades en línea de sus usuarios. Esta obligación de retención permitiría a las autoridades encargadas de hacer cumplir la ley, acceder posteriormente a estos datos en sus tareas de seguridad, investigación y persecución del delito.

Quienes proponen este tipo de políticas sostienen que en la medida en que los datos retenidos no se relacionen con el contenido de las comunicaciones electrónicas, su captura y conservación no constituyen, en sí misma, una injerencia a la vida privada de las personas ni pueden afectar el ejercicio de los derechos humanos.

La Relatoría Especial advierte que esta posición no encuentra sustento en la jurisprudencia y doctrina del sistema interamericano y del sistema universal de protección de derechos humanos, que en los últimos años ha sido enfática al afirmar que la protección a la vida privada no se limita al contenido de las comunicaciones, sino que incluye a otros aspectos propios del proceso de comunicación.

En el fallo *Escher y Otros vs. Brasil*, la Corte Interamericana de Derechos Humanos determinó que la protección del derecho a la privacidad comprende tanto las operaciones técnicas dirigidas a registrar el contenido de las comunicaciones, mediante su grabación y escucha, "como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones"[12].

En su Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, esta oficina reconoció de manera particular que los metadatos de las comunicaciones digitales, que incluyen, entre otros, la ubicación, actividades en línea, y con quiénes se comunican los usuarios de Internet, pueden ser altamente reveladores, y su recolección y conservación equivalen a una limitación directa al derecho a la intimidad y vida privada de las personas[13]. En el reciente informe *El derecho a la privacidad en la era digital*, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos indicó que desde el punto de vista del derecho a la privacidad, "[l]a agregación de la información comúnmente conocida como 'metadatos' puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias

[12] Corte IDH. *Caso Escher y otros Vs. Brasil.* Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200, párr. 114.

[13] Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos (OEA) y Relator Especial de las Naciones Unidas (ONU) para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión. 21 de junio de 2013. *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*.

privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada"[14].

En esa medida la Relatoría Especial ha expresado seria preocupación por la adopción de políticas que obligan a los proveedores de servicios de Internet y de telecomunicaciones a retener los metadatos de las comunicaciones para la práctica de vigilancia histórica – en contraposición a mecanismos de retención selectivos y limitados claramente por ley –. Al respecto, en la Declaración conjunta sobre la libertad de expresión y las respuestas a las situaciones de conflicto, adoptada el 3 de mayo de 2015, los Relatores Especiales de la ONU, OSCE, OEA, y de la Comisión Africana afirmaron que la "obligación de retener o las prácticas de retención de datos personales de forma indiscriminada con el fin de mantener el orden público o por motivos seguridad no son legítimos. En cambio, los datos personales deberían ser retenidos con fines de orden público o para temas de seguridad solo de forma limitada y selectiva y en una forma que represente un equilibrio adecuado entre los agentes del orden público y la seguridad y los derechos a la libertad de expresión y a la privacidad"[15].

En su informe sobre las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y expresión, el Relator Especial de las Naciones Unidas (ONU) para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Frank La Rue, indicó que "la conservación obligatoria de datos está facilitando la recopilación a gran escala de datos que luego pueden refinarse y analizarse". El Relator afirmó que estas políticas "son invasivas y costosas, y atentan contra los derechos a la intimidad y la libre expresión. Al obligar a los proveedores de servicios de comunicaciones a generar grandes bases de datos acerca de quién se comunica con quién telefónicamente o por Internet, la duración del intercambio y la ubicación de los usuarios, y a guardar esta información (a veces durante varios años), las leyes de conservación obligatoria de datos aumentan considerablemente el alcance de la vigilancia del Estado, y de este modo el alcance de las violaciones de los derechos humanos. Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental"[16]. En este informe, el Relator recomendó a los Estados no exigir la retención de información determinada puramente con fines de vigilancia.

Los riesgos de acceso ilícito de estos datos y la obligación concreta de establecer límites robustos a este tipo de políticas fueron analizados también por la Corte Europea de Justicia en el fallo *Digital Rights Ireland Ltd* de 8 de abril de 2014, en el que declaró inválida la Directiva 2006/24 del Parlamento Europeo y del Consejo de la Unión sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas[17]. En su decisión, la Corte Europea de Justicia reconoció que los "datos relativos al uso de comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en la prevención de delitos y la lucha contra la delincuencia, en especial la delincuencia organizada". Afirmó que "la conservación de datos para su eventual acceso por parte de las autoridades nacionales competentes que impone la Directiva 2006/24 responde efectivamente a un objetivo de interés general".

[14] Naciones Unidas. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos El Derecho a la Privacidad en la Era Digital. A/HRC/27/37. 30 de junio de 2014. Párr. 19.

[15] Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relator Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). 3 de mayo de 2015. *Declaración conjunta sobre la libertad de expresión y las respuestas a las situaciones de conflicto*

[16] Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40. 17 de abril de 2013.

[17] Tribunal Europeo de Justicia (Gran Sala). 8 de abril de 2014. Digital Rights Ireland Ltd e Irlanda. Comunicaciones electrónicas — Directiva 2006/24/CE — Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones — Conservación de datos generados o tratados en relación con la prestación de tales servicios — Validez — Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea.

No obstante, estableció que este tipo de normativa "debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos". Al examinar la Directiva en cuestión, la Corte Europea observó que no reunía los siguientes límites o garantías:

a) Limitar la retención a datos relacionados con un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, o a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves.

b) Establecer excepciones respecto de personas cuyas comunicaciones están sujetas al secreto profesional con arreglo a las normas de la legislación nacional.

c) Establecer los periodos de retención en función a la posible utilidad de distintas categorías de datos para el objetivo perseguido o de las personas afectadas. En todo caso, la determinación del período de conservación debe basarse en criterios objetivos para garantizar que ésta se limite a lo estrictamente necesario.

d) Supeditar el acceso a los datos a un control judicial previo, o a la revisión de autoridades administrativas independientes.

e) Establecer criterios objetivos que permitan delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delito. Por ejemplo, precisar las condiciones materiales y de procedimiento correspondientes.

f) Definir expresamente que el acceso y la utilización posterior de los datos de que se trata deberán limitarse estrictamente a fines de prevención y detección de delitos graves delimitados de forma precisa o al enjuiciamiento de tales delitos.

g) Limitar el número de personas que disponen de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el objetivo perseguido.

h) Garantizar que los proveedores de servicios de comunicaciones electrónicas apliquen un nivel especialmente elevado de protección y seguridad de los datos conservados a través de medidas técnicas y organizativas.

i) Garantizar la destrucción definitiva de los datos al término de su período de conservación.

j) Asegurar que los datos conservados se mantengan en el territorio de la Unión Europea.

Sobre la base de estas consideraciones, la Corte Europea de Justicia determinó que la Directiva "sobrepasó los límites que exige el respeto del principio de proporcionalidad", es decir, rebasó los límites de lo que se considera necesario para el logro de los objetivos perseguidos.

En suma, si un Estado llegase a determinar que el establecimiento de leyes que obligan a los proveedores de servicios de telecomunicaciones e Internet la retención de datos de las comunicaciones electrónicas resulta verdaderamente necesaria a fines de la prevención, investigación y enjuiciamiento de delitos graves, deberá asegurar que se trata de una retención limitada y selectiva en función a lo estrictamente necesario según el objetivo perseguido.

Teniendo en cuenta lo anterior, la Relatoría Especial solicita respetuosamente al Gobierno de Su Excelencia suministrar, dentro del plazo de 15 días hábiles contados a partir de la fecha de transmisión de la presente comunicación, la información que estime pertinente sobre el Decreto Legislativo No. 1182. En particular, se le solicita información sobre:

a) Las razones que llevaron al Estado a impulsar esta legislación.

b) El nivel de participación de la sociedad civil en la formulación del Decreto Legislativo.

c) Los límites de proporcionalidad impuestos, si los hubiere, para asegurar su compatibilidad con el derecho internacional de los derechos humanos en esta materia.

d) Si el Estado planea revisar la legislación, y de ser el caso, bajo qué condiciones.

De igual forma, con el fin de apoyar los esfuerzos de su Ilustre Estado en regular adecuadamente los asuntos objeto de tratamiento en el Decreto Legislativo de referencia, rogamos a su Excelencia hacer llegar esta comunicación a las autoridades nacionales competentes, incluidos el Ministerio Publico y la Policía Nacional, así como los Poderes Judiciales y Legislativos.

Aprovecho la oportunidad para expresar a Su Gobierno el testimonio de mi más alta y distinguida consideración.

Edison Lanza
Relator Especial para la Libertad de Expresión
Comisión Interamericana de Derechos Humanos
Organización de Estados Americanos