RELATORÍA ESPECIAL PARA LA LIBERTAD DE EXPRESIÓN

Estimada Señora Nathalie Prouvez
Jefe de la Sección de Estado de Derecho y Democracia
Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH)

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) tiene el honor de dirigirse a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), con el objeto de transmitirle la presente carta relacionada con la comunicación enviada el 30 de agosto del 2019 por su Oficina, mediante la cual solicita insumos para el Informe Temático "sobre las nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, y su impacto en la promoción y protección de los derechos humanos en el contexto de las asambleas, incluidas las protestas pacíficas".

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) aprovecha la oportunidad para expresar a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos el testimonio de su más alta y distinguida consideración.

Washington, D.C. 16 de octubre de 2019

Cordialmente,

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

RELATORÍA ESPECIAL PARA LA LIBERTAD DE EXPRESIÓN

16 de octubre de 2019

Ref: Insumos de la Relatoría Especial para la Libertad de Expresión de la CIDH para el Informe sobre "Nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, y su impacto en la promoción y protección de los derechos humanos en el contexto de las protestas".

Estimada Señora Nathalie Prouvez:

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) con relación a la comunicación enviada el 30 de agosto del 2019 por su Oficina a la Comisión Interamericana, en la cual solicita insumos para el Informe Temático "sobre las nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, y su impacto en la promoción y protección de los derechos humanos en el contexto de las asambleas, incluidas las protestas pacíficas".

Agradezco esta importante oportunidad para colaboración con la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH). En esta nota se abordará, en primer lugar, los estándares desarrollados por la CIDH y su Relatoría Especial para la Libertad de Expresión en el informe aprobado en 2019 sobre "Protestas y Derechos Humanos", en el capítulo sobre "Protestas e Internet. Seguidamente, se hará referencia al uso de nuevas tecnologías, incluida la tecnología de la información y las comunicaciones, en el contexto de las asambleas, incluidas las protestas pacíficas, sobre las cuales se hizo mención en el Informe "Protestas y Derechos Humanos"; y se señalarán algunos ejemplos de casos concretos en la región que fueron documentados por esta Oficina en los últimos anos.

Finalmente, esta Relatoría Especial hace referencia a su Informe temático sobre "Estándares para una Internet libre, abierta e incluyente", de 2017, en el cual esta Oficina abordó, entre otros, la temática de "Internet y la protección de la privacidad", temática que puede ser de relevancia para su Informe Temático.

1. **Los desafíos a los derechos humanos generados por las interferencias con la disponibilidad y el uso de tecnologías en el contexto de las asambleas, incluidas las protestas pacíficas (por ejemplo, a través de interrupciones de la red, bloqueo de servicios de Internet o restricciones en comunicaciones seguras y confidenciales).**

En su reciente informe aprobado por la CIDH en 2019 sobre "Protesta y Derechos Humanos", pendiente de publicación[1], la Relatoría Especial abordó la temática de las interferencias con la disponibilidad y el uso de tecnologías en el contexto de las protestas pacíficas en el capítulo sobre "Protestas e Internet". En esa oportunidad, esta Oficina señaló que:

Internet actualmente constituye una herramienta fundamental de comunicación que permite a las personas vincularse y conectarse de manera ágil, veloz y efectiva, y es considerada una herramienta con un potencial único para el ejercicio de la libertad de expresión. Entre las nuevas potestades que internet habilita destacan la habilidad para asociarse y reunirse que las personas adquieren en la era digital y que potencia, a su vez, la plena realización y el goce de otros derechos civiles, políticos, económicos, sociales y culturales. Las

[1]La publicación del Informe sobre "Protesta y Derechos Humanos" está prevista para el 6 de noviembre de 2019 y será enviado a esa Oficina tan pronto esté disponible.

reuniones y asociaciones en la era digital pueden ser organizadas y celebradas sin anticipación previa, con poco tiempo y bajo costos. Además, constituye actualmente una herramienta fundamental para el control y la denuncia de violaciones a los derechos humanos durante manifestaciones y reuniones.

Internet puede verse y analizarse como medio de organización o como plataforma habilitante de las protestas[2]. En la práctica funciona como un medio de difusión, convocatoria y publicidad de reuniones y asociaciones físicas (utilizando redes sociales, blogs, o foros, por ejemplo), expandiendo las fronteras de la participación, para ser llevada a cabo en un lugar público tangible; por otro lado internet ofrece la posibilidad de organizar una protesta en línea, proveyendo un espacio de encuentro común, acortando distancias y tiempos, simplificando formalidades y agendas. Ambas instancias han de ser protegidas y promovidas en la medida en que coadyuvan al pleno ejercicio de los derechos humanos.

Los estándares internacionales desarrollados en el seno del sistema interamericano y del sistema universal sobre los derechos a la libertad de expresión, a asociación y reunión pacífica tienen plena vigencia en internet.

En los últimos años se han dado distintas instancias de protesta en internet que incluyen cadenas de emails, peticiones, manifestaciones y campañas desarrolladas en redes sociales, etc. De la misma manera como los Estados deben asegurar el acceso a espacios públicos, tales como calles, carreteras y plazas públicas para la celebración de reuniones, deben también asegurar que internet se encuentre disponible y sea accesible para todos los ciudadanos para poder ser un espacio que permita la organización de asociaciones y reuniones con el fin de participar en la vida política del país.

Las limitaciones en el acceso a internet, incluyendo las desconexiones totales o parciales, la ralentización de internet, los bloqueos temporales o permanentes de distintos sitios y aplicaciones, antes durante o después de reuniones pacificas constituyen restricciones ilegitimas a los derechos de asociación y reunión. El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión de Naciones Unidas hizo hincapié en la necesidad de asegurar el acceso a internet en todo momento, también en los períodos de malestar político[3].

En ningún caso la mera participación en protestas, en su difusión u organización puede motivar la violación del derecho a la privacidad respecto de las comunicaciones privadas realizadas por una persona, ya sean realizadas por escrito, por voz o imágenes, y con independencia de la plataforma utilizada. El derecho a la privacidad abarca no solamente las comunicaciones individuales, sino también las comunicaciones que se desarrollan en grupos cerrados a los que solo los miembros tienen acceso.

Se ha denunciado en la región la presencia en las redes sociales de agentes policiales y militares infiltrados o con identidades falsas con el objetivo de obtener información sobre movimientos sociales y la organización de manifestaciones y protestas. Dicha práctica puede ser considerada una violación grave de los derechos de reunión y libertad de asociación, e incluso del derecho de privacidad. En ninguna circunstancia se encuentran permitidas acciones de inteligencia en internet para vigilar a los organizadores o participantes de protestas sociales.

Los Estados deben permitir y fomentar el uso abierto y libre de internet, así como de todas las demás formas de comunicación y las excepciones a dicho acceso han de estar claramente establecidas en la ley y cumplir con el test tripartito establecido en el sistema interamericano. Las leyes que regulan los denominados "ciberdelitos" han de estar clara y específicamente redactadas garantizando el principio de legalidad, tener un fin legítimo, ser necesarias en una sociedad democrática y ser proporcionadas y en ningún caso han de ser utilizadas para prohibir, obstaculizar o entorpecer una reunión, manifestación o protesta pacífica.

[2] General Assembly. Human Rights Council. Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of Association. A/HRC/41/41. 17 May 2019.

[3] General Assembly. Human Rights Council. Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of Association. A/HRC/41/41. 17 May 2019.

La garantía de la privacidad y el anonimato también forman parte de los derechos de asociación y reunión. Sin perjuicio de lo cual, no ampara todo tipo de expresiones o asociaciones. Por el contrario, "el anonimato del emisor de ninguna manera protegería a quien difunda pornografía infantil, a quien hiciera propaganda a favor de la guerra o apología del odio que constituya incitación a la violencia o incitare pública y directamente al genocidio". Los Estados deben garantizar la plena protección del discurso anónimo y regular los casos y condiciones específicas cuando dicho anonimato deba ser levantado, requiriendo para ello control judicial suficiente y la plena vigencia del principio de proporcionalidad respecto de las medidas tendientes a identificar a la persona en cuestión.

2. Los desafíos de derechos humanos planteados por el uso de nuevas tecnologías, incluida la tecnología de la información y las comunicaciones, en el contexto de las asambleas, incluidas las protestas pacíficas (por ejemplo, el uso de herramientas de vigilancia y monitoreo por parte de las autoridades, incluida la tecnología de reconocimiento basada en biometría para identificar a los manifestantes);

En su reciente informe aprobado por la CIDH en 2019 sobre "Protesta y Derechos Humanos", esta Relatoría Especial señaló que "[l]a Comisión cree relevante que se ponga atención al desarrollo de tecnologías de sistemas sin operadores controlados a distancia (como por ejemplo los drones). Este nuevo campo de desarrollo tecnológico es pasible de ser utilizado en el contexto de manifestaciones sociales o en el control de multitudes. De acuerdo a lo señalado por el Relator de Ejecuciones Extrajudiciales: 'La disponibilidad de tecnología avanzada lleva aparejada un aumento de los niveles de obligación, tanto respecto de las decisiones sobre si se debe usar la fuerza y en qué medida como de la rendición de cuentas y la supervisión en relación con el ejercicio de esa facultad discrecional'"[4].

2.1 Ejemplos de casos concretos en la región documentados por la Relatoría Especial en los últimos años:

En 2015, la Relatoría Especial envió a solicitud de una Senadora de **Paraguay**, una nota técnica sobre el Proyecto de Ley que establecía la obligación de conservar datos de tráfico, y que en ese momento se encontraba en discusión en el Congreso Nacional del país. Según la información recibida, mencionado Proyecto de Ley tenía por objeto "regular la conservación de datos de tráfico por parte de personas físicas o jurídicas que proveen Servicios de Acceso internet y Transmisión de Datos" y el deber de "proporcionar esos datos con autorización del juez de garantías, cuando lo requieran, con la finalidad de investigar, perseguir y sancionar a los responsables de los hechos punibles tipificados en el Código Penal Paraguayo y en otras leyes penales especiales".

En respuesta a esta solicitud, esta Oficina reiteró al Gobierno paraguayo algunos aspectos del derecho internacional de los derechos humanos que resultaba relevante que el Estado tuviese en cuenta al momento de debatir dicho proyecto de ley. En particular, en esta comunicación se puso 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. A continuación, indicamos los estándares que fueron señalados al Estado en esa nota técnica:

- **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.

[4]ONU Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Nota del Secretario General, A/69/265, 6 Agosto 2014 párr. 67.

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.

Al respecto, como ya ha sido expuesto por esta Oficina, 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 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.

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), 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.

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.

- **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".

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

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".

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". 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. 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".

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 administrativasindependientes.

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.

Al igual que en el régimen europeo descrito, en el marco jurídico interamericano cualquier restricción legítima del derecho a la libertad de expresión y el derecho a la privacidad en Internet 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 expresó esta Oficina en su Informe sobre Libertad de Expresión e Internet, 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".

En efecto, este tipo de medidas debe encontrarse establecida por medio de leyes en sentido formal y material. Dichas leyes deben ser claras y precisas. 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". Ello resulta particularmente relevante dado el extraordinario volumen, variedad y complejidad de los datos personales afectados por una política de retención obligatoria de datos electrónicos.

Finalmente, 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. 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.

Por otra parte, en julio de 2017, la Relatoría Especial publicó un comunicado de prensa a través del cual manifestó su preocupación ante denuncias sobre espionaje de periodistas y defensores de derechos humanos en **México** e instó el Estado a desarrollar una investigación completa e independiente sobre estos hechos. Según información difundida por un conjunto de organizaciones de la sociedad civil, entre enero de 2015 y agosto de 2016, se habrían registrado 97 intentos de infección de los teléfonos portátiles de periodistas, defensores de derechos humanos, abogados y políticos con un software malicioso (malware) de espionaje, conocido como "Pegasus". De acuerdo con la información revelada, el malware afectaría al teléfono inteligente, permitiendo "el acceso a los archivos guardados en el equipo, así como a los contactos, mensajes, correos electrónicos. El malware también obtiene permisos para usar, sin que el objetivo lo sepa, el micrófono y la cámara del dispositivo". Los hechos también fueron informados e investigados por el diario *The New York Times* y expertos informáticos independientes.

Entre las 19 personas que habrían sido objeto de intentos de infección con "Pegasus" en México, se encuentran los periodistas Carmen Aristegui y Carlos Loret de Mola, los defensores Mario Patrón, Santiago Aguirre y Stephanie Brewer del Centro de Derechos Humanos Miguel Agustín Pro Juárez (Centro PRODH) y al menos un integrante del Grupo Interdisciplinario de Expertos Independientes (GIEI), creado mediante un acuerdo firmado en noviembre de 2014 por la CIDH, el Estado mexicano y representantes de los 43 estudiantes desaparecidos en Ayotzinapa. Al momento de los ataques denunciados, las víctimas investigaban e informaban sobre hechos de marcado interés público y/o desarrollaban acciones de defensa de graves violaciones a los derechos humanos.

Durante la audiencia sobre Justicia e Impunidad en México, celebrada el jueves 6 de julio de 2017 en el 163 periodo de sesiones de la CIDH, las organizaciones de derechos humanos participantes expresaron su alarma por las denuncias de espionaje a personas críticas al gobierno mexicano. Estimaron además que la Procuraduría General de la República (PGR) "no puede garantizar una investigación imparcial y autónoma", dado que su agencia de investigación criminal es una de las entidades que habría adquirido el referido malware. En tal sentido, afirmaron que "la única ruta posible hacia la justicia es por medio de la conformación de un panel internacional de expertas y expertos". Igualmente, durante la audiencia sobre el Mecanismo Especial de Seguimiento de Ayotzinapa, México, también celebrada por la CIDH en su 163 período de sesiones, el Centro PRODH denunció los intentos de espionaje en contra de miembros de esa organización. En estas audiencias, el Estado indicó que la Fiscalía Especial para la Atención de Delitos Cometidos contra la Libertad de Expresión (Feadle) de la PGR inició una investigación por estos hechos y que los denunciantes han sido invitados a rendir declaraciones y otros elementos necesarios para adelantar la investigación. Asimismo, informó que la Feadle ha propuesto establecer una colaboración con agencias nacionales e

internacionales para "fortalecer cualquier investigación y determinar, de ser el caso, las responsabilidades correspondientes".

La Relatoría Especial tomó nota que el 21 de junio de 2017, mediante comunicado de prensa DGC/203/17, la Comisión Nacional de Derechos Humanos de México informó que requirió a distintas dependencias del gobierno federal (entre ellas la Secretaría de la Defensa Nacional SEDENA, la Secretaría de Marina SEMA, el Centro de Investigación y Seguridad Nacional y la PGR) a "implementar acciones para que en caso de poseer programas para intervenir comunicaciones de aparatos telefónicos y computadoras, se abstengan de emplearlo contra periodistas, organizaciones de la sociedad civil y defensores de derechos humanos, así como contra cualquier otra persona contraviniendo el orden jurídico constitucional". A su vez, se solicitó que, "en caso de haberse obtenido información mediante este tipo de programas, se abstengan de utilizarla o difundirla y sea valorada su legalidad por las instancias competentes" y que se "realice la investigación de los hechos con profesionalismo, exhaustividad, objetividad y diligencia". Asimismo, esta Oficina observó que el Estado mexicano, a través de un comunicado conjunto de 10 de julio de 2017, expresó su "rechazo a cualquier acto que atente en contra de la libertad de expresión y del derecho a la privacidad de las personas".

Adicionalmente, en su Informe Anual de 2018 "Conexión Incierta #Derechos DigitalesIPYSve", el Instituto Prensa y Sociedad (IPYS) **Venezuela**, señaló, entre otros, que en Venezuela se observó en 2018 "acciones legales y medidas de censura que coartaron la expresión de periodistas y ciudadanos a través de plataformas digitales, limitaciones de acceso a internet por fallas de infraestructura, los hechos de intimidación y ataques en la red y bloqueos a portales de medios de comunicación digitales y de organizaciones no gubernamentales, limitaciones a la privacidad, así como declaraciones agraviantes en las redes sociales por parte de autoridades públicas"[5].

En 2018, asimismo, en el Capítulo sobre **Nicaragua** de su Informe Anual, la Relatoría Especial indicó que las redes sociales e internet continuarían siendo en el país un medio alternativo a través del cual las personas podían divulgar información de interés público, manifestar y expresar ideas y opiniones de toda índole. No obstante, indicó que de acuerdo con la información recibida, un grupo afín al gobierno se dedicaría a desinformar a través de estas redes y estigmatizar a periodistas y medios de comunicación que transmiten información crítica contra el gobierno nicaragüense. Asimismo, señaló que durante la visita de trabajo al país la CIDH recibió testimonios que denunciaban que el gobierno ordenó monitorear los perfiles de las redes sociales con la finalidad de conocer quiénes participaron en las protestas o difundieron mensajes o informaciones contrarias al gobierno. La CIDH observó con preocupación que estas personas podrían ser objeto de represalias por parte de las autoridades. Además, señaló que previo a la crisis iniciada el 18 de abril, la Relatoría Especial recibió información sobre intenciones del gobierno de presentar un proyecto de ley que buscaría controlar las redes sociales por casos de "cyber-acoso"[6].

También en 2018, se recibió información que daba cuenta que **el Estado de Guatemala** habría adquirido software y equipos técnicos que poseen la capacidad de interceptar móviles telefónicos, así como cuentas de redes sociales. En este contexto, esta tecnología habría sido utilizada con la finalidad de interceptar móviles y redes sociales de políticos, periodistas, diplomáticos y dirigentes sociales, así como se habrían empleado técnicas de vigilancia dirigidas a determinadas personas. De acuerdo con información de público conocimiento, estos equipos habrían sido adquiridos con fondos de la Dirección General de Inteligencia Civil (Digici) que depende orgánicamente del Ministerio de Gobernación. Además, desde la Digici se habría llevado a cabo los hechos de interceptación. Otros equipos habrían sido adquiridos con fondos de la Policía Nacional Civil (PNC) y también de la Secretaría de Inteligencia del Estado. Según la información disponible, se habrían adquirido equipos tecnológicos como Circles, y programas como Pegasus, Pen-Link, Laguna, Citer 360, entre otros, que poseen la capacidad de interceptar llamadas, desencriptar mensajes, extraer datos de llamadas, entre otras capacidades. Asimismo, para la adquisición de estos programas se habrían diseñado contratos en cuyas especificaciones técnicas figurarían informaciones generales descriptas

[5] IPYS Venezuela. Conexión incierta – Informe Annual Derechos Digitales IPYSve de 2018. 17 de mayo de 2019.

[6] CIDH. Informe Anual 2018. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo II (Situación de la Libertad de Expresión en el hemisferio). OEA/Ser.L/V/II. Doc. 30. 17 de marzo de 2019. Párr. 779.

como "seguridad del Estado"[7]. Según lo informado, el Ministro de Gobernación, Enrique Degenhart, habría manifestado que no existen capacidades para interceptar correos y llamadas[8] y que esas herramientas habrían sido adquiridas en gobiernos anteriores y secuestradas con orden judicial por el Ministerio Público y la Comisión Internacional contra la Impunidad por lo que ellos tendrían conocimiento del uso de dichas herramientas en la actualidad[9]. Asimismo, la Procuraduría de los Derechos Humanos (PDH) habría abierto un expediente de oficio por los posibles hechos de espionaje por parte del gobierno a empresarios, políticos, periodistas, diplomáticos y dirigentes sociales[10].

Finalmente, en 2019, esta Oficina fue informada que el 18 de marzo, fue presentado un nuevo Sistema de Vigilancia Móvil en la Región Metropolitana de Santiago, **Chile**, que mediante el uso de drones y cámaras buscaría combatir la delincuencia y ayudar en la coordinación de las distintas autoridades regionales y comunales en el trabajo conjunto y eficiente para mejorar la seguridad. De acuerdo con la información disponible, las aeronaves no tripuladas estarían equipadas con cámaras de alta definición para obtener información visual y transmitirla en vivo a centrales de monitoreo ubicadas en las intendencias regionales, donde operadores capacitados observarían las imágenes que entregan los drones. Fue informado, asimismo, que ayudadas por las cámaras de alta definición, las aeronaves contarían con programas computacionales que les permitirían hacer reconocimiento facial automatizado. Además de las aeronaves en la Región Metropolitana, se habría implementado un programa piloto en Antofagasta en diciembre de 2018, y se planea la extensión durante el presente año a las regiones de Coquimbo, Valparaíso, Biobío y La Araucanía; y el resto del país se aplicará en 2020.

Sobre el particular, esta Oficina señala que el ejercicio en los espacios públicos de los derechos a reunirse pacíficamente y a asociarse con otros son habilitantes para el ejercicio de la libertad de expresión, y en tanto, derechos fundamentales se refuerzan mutuamente de manera natural. En este sentido, un riesgo aumentado de enfrentar tanto la persecución criminal como la acción policial, facilitados por una vigilancia más intrusiva, son disuasivos significativos contra el ejercicio de estos derechos. De este modo, el monitoreo, registro y almacenamiento de las actividades regulares de personas y organizaciones que realizan manifestaciones y protestas en el espacio público constituye una injerencia indebida en el ámbito de la privacidad, salvo que por una razón fundada sea aprobada por el poder judicial.

Sobre los programas de vigilancia *per se*, esta Oficina ha señalado que estos deben ser diseñados e implementados atendiendo a los estándares internacionales en materia de derechos humanos. Particularmente, los Estados deben garantizar que la intervención, recolección y uso de información personal, incluidas todas las limitaciones al derecho de la persona afectada a acceder a información sobre las mismas, estén claramente 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. Asimismo, la ley debe autorizar el acceso a las comunicaciones y a datos personales solo en las circunstancias más excepcionales definidas en la legislación[11].

Asimismo, la Relatoría ha observado que 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; si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario y si

[7] Nómada GT. 6 de agosto de 2018. *Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)* (reproducción autorizada de artículo de "Nuestro Diario").

[8] Soy502. 6 de agosto de 2018. *Investigación revela cómo el Gobierno espió a los guatemaltecos*; Cuenta de Twitter de Roberto Caubilla @RobertoCSOy502. 6 de agosto de 2018; El Nuevo Herald. 6 de agosto de 2018. *Gobierno de Guatemala niega espionaje informático*.

[9] La Hora. 6 de agosto de 2018. *Reportaje de ND denuncia escuchas ilegales del Estado; Degenhart lo niega y encima acusa*.

[10] Publisnews. 6 de agosto de 2018. *PDH abre expediente por las denuncias de espionaje del gobierno*; Impacto. 6 de agosto de 2018. *PDH abre de oficio expediente por posible espionaje del Gobierno*; Cuenta oficial de Twitter de la Procuraduría de los Derechos Humanos de Guatemala @PGHgt. 6 de agosto de 2018.

[11] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo II (Evaluación sobre el estado de la Libertad de Expresión en el Hemisferio). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. Párr. 415.

resulta proporcional respecto del interés que se quiere promover. Finalmente, la Relatoría observa que por lo menos los criterios de decisión adoptados por los tribunales deberían ser públicos[12].

3. Conclusiones

Agradezco a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) la posibilidad de pronunciarme sobre el asunto en cuestión y espero que estos insumos contribuyan al Informe "sobre las nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, y su impacto en la promoción y protección de los derechos humanos en el contexto de las asambleas".

En tal sentido, la Relatoría Especial para la Libertad de Expresión de la CIDH reitera la plena disposición para colaborar y acompañar las iniciativas relacionadas con la temática.

Aprovecho la oportunidad para expresar 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

[12] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo II (Evaluación sobre el estado de la Libertad de Expresión en el Hemisferio). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. Párr. 416.