RECOMENDACIÓN GENERAL No. 47/2022 "AUSENCIA DE REGULACIÓN JURÍDICA PARA LA ADQUISICIÓN Y USO DE TECNOLOGÍAS PARA LA VIGILANCIA, INTERVENCIÓN Y RECOLECCIÓN DE DATOS DE PERSONAS EN TERRITORIO NACIONAL: SU IMPACTO EN LA LIBERTAD DE EXPRESIÓN, EL DERECHO A DEFENDER DERECHOS HUMANOS Y SU VINCULACIÓN AL DEBER DE CUIDADO A CARGO DEL ESTADO MEXICANO".

Ciudad de México, a 24 de mayo de 2022

SEN. OLGA MARÍA DEL CARMEN SÁNCHEZ CORDERO DÁVILA
PRESIDENTA DE LA MESA DIRECTIVA DE LA CÁMARA DE SENADORES
DEL CONGRESO DE LA UNIÓN

DIP. SERGIO CARLOS GUTIÉRREZ LUNA
PRESIDENTE DE LA MESA DIRECTIVA DE LA CÁMARA DE DIPUTADOS
DEL CONGRESO DE LA UNIÓN

SEN. IMELDA CASTRO CASTRO
PRESIDENTA DE LA COMISIÓN BICAMARAL DE SEGURIDAD NACIONAL
DEL PODER LEGISLATIVO

LIC. ROSA ICELA RODRIGUEZ VELÁZQUEZ
SECRETARIA DE SEGURIDAD Y PROTECCIÓN CIUDADANA
EN SU CALIDAD DE SECRETARIA EJECUTIVA
DEL CONSEJO DE SEGURIDAD NACIONAL

DR. ALEJANDRO GERTZ MANERO
FISCAL GENERAL DE LA REPÚBLICA

1. El artículo 1°, párrafo tercero, de la Constitución Política de los Estados Unidos Mexicanos establece la obligación de todas las autoridades, en el ámbito de sus competencias, de promover, respetar, proteger y garantizar los derechos humanos, de

conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.

2. El artículo 6, fracción VIII, de la Ley de la Comisión Nacional de los Derechos Humanos (CNDH) establece como atribución de este Organismo: "Proponer a las diversas autoridades del país que, en el exclusivo ámbito de su competencia, promuevan los cambios y modificaciones de disposiciones legislativas y reglamentarias, así como de prácticas administrativas que a juicio de la Comisión Nacional redunden en una mejor protección de los derechos humanos". En tal virtud, de conformidad con lo dispuesto en el artículo 140 del Reglamento Interno de la Comisión Nacional de los Derechos Humanos, se expide la presente Recomendación General.

3. Con el propósito de proteger la información de las personas jurídicas relacionadas con los hechos y evitar que sus datos sean divulgados, se omitirá su publicidad en atención a lo dispuesto en los artículos 4o, párrafo segundo, de la Ley de la Comisión Nacional de los Derechos Humanos, y 147 de su Reglamento Interno, en relación con lo establecido en el artículo 113, fracción XII de la Ley General de Transparencia y Acceso a la Información Pública, y 110, fracción XII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que tal información se relaciona con la integración de una carpeta de investigación ante la Fiscalía General de la República que a la fecha de emisión de la presente Recomendación General se encuentra en trámite. La información se pondrá en conocimiento de las autoridades recomendadas a través de un listado adjunto, en que se describe el significado de las claves utilizadas, con el compromiso de dictar las medidas de protección de los datos correspondientes.

4. Para una mejor comprensión del presente documento, las claves y denominaciones utilizadas para distintas personas involucradas en los hechos, son las siguientes:

DENOMINACIÓN	CLAVE
Autoridad	**A**
Empresa	**E**
Organización	**O**
estigación	**CI**

5.En la presente Recomendación General la referencia a distintas dependencias, personas, instancias de gobierno, autoridades e instrumentos se hará con acrónimos o abreviaturas a efecto de facilitar la lectura y evitar su constante repetición, las cuales podrán ser identificadas como sigue:

DENOMINACIÓN	SIGLAS, ACRÓNIMO O ABREVIATURA
Centro Nacional de Inteligencia, antes Centro de Investigación y Seguridad Nacional (CISEN), cuya referencia se realiza acorde a lo establecido en el Transitorio Octavo del Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana, publicado en el Diario Oficial de la Federación el 30 de abril de 2019	**Centro**
Comisión Nacional de los Derechos Humanos	**CNDH, Comisión Nacional, Organismo Nacional, Organismo Constitucional**
Comisión Interamericana de Derechos Humanos	**CIDH**

DENOMINACIÓN	SIGLAS, ACRÓNIMO O ABREVIATURA
Corte Interamericana de Derechos Humanos	**CrIDH**
Convención Americana sobre Derechos Humanos	**Convención**
Suprema Corte de Justicia de la Nación	**SCJN**
Fiscalía Especial para la Atención de Delitos Cometidos Contra la Libertad de Expresión, de la Fiscalía General de la República	**FEADLE**

I. ANTECEDENTES

6. Los días 19 y 20 de junio de 2017, la Comisión Nacional de los Derechos Humanos recibió escritos de queja que presentaron periodistas, comunicadores y personas defensoras de derechos humanos, en los que señalaron que fueron objeto de intentos de ataques informáticos de vigilancia, vía teléfonos celulares, a través del sistema Pegasus[1], ya que entre 2015 y 2016 recibieron mensajes de texto con enlaces maliciosos que incitaban a presionar dominios que fueron identificados por la organización **O1** como causantes de la infección por el sistema Pegasus. Cabe señalar que entre las personas que recibieron tales enlaces maliciosos en el periodo indicado, se encontraba una persona menor de edad.

7. Así mismo refirieron que, a su consideración, los presuntos ataques provinieron de agentes gubernamentales, ya que existe evidencia de que agencias del Estado mexicano adquirieron herramientas sofisticadas de *hacking* o *software*[2] de vigilancia, en atención

[1] "Se trata de un software de vigilancia creado por la empresa israelí NSO Group con el objetivo de combatir el terrorismo y la delincuencia. Un software específico para gobiernos. Por tanto, una tecnología difícil de alcanzar y detectar." Tomado de: https://www.esedsl.com/blog/pegasus-que-es-y-como-funciona-este-software-de-espionaje

[2] El hacking se puede definir como: la búsqueda y explotación de vulnerabilidades de seguridad en sistemas de cómputo o redes. El Diccionario Oxford Languages, define *Software* como el "conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas".

a que en julio de 2015 la organización **O2** filtró correos electrónicos de la empresa **E1**, de los que se acreditó que el Estado mexicano compró herramientas de vigilancia y espionaje desarrolladas por esta empresa.

8. Igualmente manifestaron que la organización **O1**, dedicada a la investigación y desarrollo tecnológico de la información, señaló que autoridades mexicanas adquirieron un *software* de la empresa **E2**, responsable del desarrollo del programa Pegasus, destinado a la intervención de comunicaciones, cuya venta se realizó exclusivamente a gobiernos, ejércitos y agencias de inteligencia.

9. Añaden que **O1**, emitió un reporte detallando cómo funciona la empresa **E2** y sus herramientas de vigilancia, en el cual se señaló que el programa Pegasus funciona explotando una vulnerabilidad de seguridad inédita del sistema operativo, que a través de la infección[3] se hace un desbloqueo al dispositivo en cuestión y se instala un sofisticado *spyware*[4] que permite al interceptor tomar control de diferentes funciones del aparato, así como acceder a sus contenidos, tales como: archivos, datos del calendario, listas de contactos, contraseñas, mensajes de texto, datos de otras aplicaciones, como: Gmail, WhatsApp, Skype, Facebook, Telegram; además, escuchar llamadas realizadas por teléfono o vía WhatsApp o Viber, así como grabar activa o pasivamente, utilizando el micrófono y la cámara del dispositivo.

10. De acuerdo con el informe de **O1**, para llevar a cabo la "infección", el atacante envía mensajes que aparentan ser legítimos, estructurados bajo cierta "ingeniería social"[5] para provocar que el objetivo haga clic[6] en el enlace. En el caso particular, los quejosos manifestaron que, entre 2015 y 2016, recibieron numerosos mensajes de texto con

3 De acuerdo al informe publicado por la organización **O1**, "la infección con Pegasus" consiste en que una persona recibe un mensaje de texto con una liga de internet en su celular, y al momento de abrirlo, o "darle clic", Pegasus se instala en el teléfono celular o dispositivo electrónico y, a partir de ese momento, el interceptor a través de Pegasus puede emplear la cámara y el micrófono del celular o dispositivo en cuestión, para grabar llamadas, registrar mensajes enviados en aplicaciones de chat móvil y rastrear movimientos del usuario del dispositivo electrónico.

4 Se trata de un *software* malicioso que infecta un ordenador o dispositivo móvil y recopila información personal, de navegación y/o de uso habitual de internet, así como otros datos.

5 R. Kissel (2012), se refiere a "ingeniería social" como el intento de engañar a alguien para obtener información que podría ser utilizada posteriormente, a fin de cometer algún ataque a la red o a los sistemas informáticos de la organización. *Glossary of key information security terms (draft)*, EUA: National Institute of Standards and Technology, DOI: http://dx.doi.org/10.6028/NIST.IR.7298.

6 Se refiere a pulsar u oprimir en el dispositivo electrónico sobre la liga (enlace) para que se redireccione a la página virtual del sitio que específica dicho enlace.

enlaces maliciosos vinculados a la infraestructura de Pegasus, mismos que fueron documentados por **O1** en el informe en cita. En dicho documento **O1** destacó que, para llevar a cabo la infección, el atacante debe asegurarse de engañar al objetivo, para lo cual los dominios empleados por **E2** buscan suplantar a otros sitios legítimos como medios de comunicación, servicios de telecomunicaciones, redes sociales, portales de gobierno, organizaciones humanitarias, aerolíneas, entre otros.

11. Adicionalmente, los quejosos manifestaron que se publicaron reportajes de contratos entre **A1** y la empresa **E3** para la adquisición de un sistema de espionaje que incluía el programa Pegasus, así como un correo electrónico en el que la empresa **E4** comunicó a la empresa **E1** la venta de Pegasus a una institución del Gobierno mexicano.

12. De igual forma, señalaron que la presunción relativa a que instituciones del Gobierno mexicano pudieron haber adquirido el programa Pegasus, se dio por las constantes menciones realizadas en diversos reportajes sobre correos filtrados de **E1**, en los que se señaló a **E2** como proveedor de equipo de espionaje.

13. Entre 2015 y 2016 los quejosos recibieron diversos mensajes de texto con intentos de infección posiblemente asociados a Pegasus. Los periodos en que recibieron tales mensajes coinciden con coyunturas críticas del trabajo que desarrollaban, por lo que consideraron que esos mensajes de texto que les fueron enviados a sus dispositivos provienen del programa Pegasus.

14. Con el objetivo de allegarse mayores datos relacionados con los hechos, este Organismo Nacional solicitó información a: ex inspector general de la Comisión Nacional de Seguridad; Director Jurídico de Petróleos Mexicanos; Secretario Técnico del Consejo Nacional de Seguridad Pública; Comisionado Presidente del Instituto Federal de Telecomunicaciones; Coordinadora Nacional Antisecuestros; titular de la Unidad de Asuntos Jurídicos de la Auditoría Superior de la Federación; Secretario de la Defensa Nacional; Secretario de Marina; titular del entonces Centro de Investigación y Seguridad Nacional, así como a los fiscales generales y secretarios generales de Gobierno de las 32 entidades federativas.

II. SITUACIÓN JURÍDICA

15. Periodistas, comunicadores y personas defensoras de derechos humanos, manifestaron a este Organismo Nacional que existe evidencia de que agencias del Gobierno mexicano han adquirido durante los últimos años, herramientas sofisticadas de *software* de espionaje, de acuerdo al contenido de diversas publicaciones[7], y que entre enero de 2015 a julio de 2016, recibieron mensajes de texto con enlaces presuntamente maliciosos hacia la infraestructura del programa Pegasus, en fechas que coinciden con situaciones coyunturales del trabajo que cada uno desarrollaba.

16. Que dichos casos se encuentran documentados en diversos informes y artículos periodísticos, en los que se expone que uno o más clientes gubernamentales de la empresa **E2** en México son operadores probables[8].

17. Con motivo de lo anterior el 19 junio de 2017, periodistas, comunicadores y personas defensoras de derechos humanos, presentaron denuncia en la entonces Procuraduría General de la República, hoy Fiscalía General de la República, radicándose la **CI**, por los delitos de acceso ilícito a sistemas y equipos de cómputo e intervención de comunicaciones privadas sin mandato judicial, previstos y sancionados en los artículos 211, Bis 1, párrafo segundo, y 177 del Código Penal Federal, misma que a la fecha de emisión de la presente Recomendación General se encuentra en integración.

III. OBSERVACIONES

18. La CNDH cuenta con información de la que se advierte que autoridades del gobierno federal efectivamente adquirieron Pegasus en el periodo de 2011 a 2017, que a pesar de la potencialidad lesiva de dicho sistema, no tomaron medida alguna que les permitiera contener el riesgo y prevenir las posibles violaciones a derechos humanos que su

7 La localización de las publicaciones aludidas en el presente apartado se ha resguardado en la hoja de claves por tratarse de información que contiene datos personales que obran en fuentes públicas, lo anterior de acuerdo al criterio 13/09 emitido por el INAI.
8 En aplicación del criterio 13/09 del INAI, la localización de las fuentes señaladas se ha resguardado en la hoja de claves.

posesión y uso implica, ya que si bien existen disposiciones normativas relacionadas con la intervención de comunicaciones privadas, éstas son normas de carácter discrecional, cuya aplicación puede ser arbitraria, debido a que no incorporan disposiciones sobre el uso, alcances y límites de tecnologías para la vigilancia, intervención y recolección de datos.

19. Bajo esa tesitura, en la presente Recomendación General se abordará la problemática que deriva de la existencia de normas generales, ambiguas y/o deficientes, que propician la posibilidad de injerencias ilegales y arbitrarias en la vida privada, no solo de personas periodistas y defensoras de derechos humanos, sino de cualquier persona que se encuentre en territorio nacional, y se realizan propuestas a fin de que las diversas autoridades a quienes se dirige la presente Recomendación General, en el ámbito de sus atribuciones, realicen las acciones para atender, resolver y prevenir la sensible problemática.

20. Lo anterior, en atención a que el artículo 16, párrafos primero y décimo segundo, de la Constitución Política de los Estados Unidos Mexicanos prevé que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento, especificando que las comunicaciones privadas son inviolables, por lo que cualquier acto que atente contra la libertad y privacidad de las mismas, debe ser sancionado penalmente.

21. Así mismo el artículo 2, apartados 1 y 2, en relación con lo previsto en el artículo 17, apartados 1 y 2 del Pacto Internacional de Derechos Civiles y Políticos; artículos 1, 2 y 11, apartados 2 y 3, de la Convención Americana sobre Derechos Humanos, establecen la obligación de los Estados de respetar y garantizar a todas las personas los derechos humanos previstos en dicho instrumento, así como emitir las disposiciones legislativas y de cualquier otra índole para hacer cumplir tales derechos, particularmente el relativo a no ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su

domicilio o su correspondencia, injerencias y/o ataques en contra de las cuales tiene derecho a ser protegidos.

22. Adicionalmente, el artículo 6, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, en relación con lo dispuesto en el artículo 13, apartados 1 y 3 de la Convención Americana sobre los Derechos Humanos, así como los artículos 1, 2 apartados 1 y 2, y 3, de la Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos, prevén el pleno ejercicio del derecho a la libertad de expresión y el derecho a defender derechos humanos, así como la responsabilidad y deber de los Estados de proteger, promover y hacer efectivos todos los derechos humanos y las libertades fundamentales, entre otras cosas adoptando las medidas necesarias para su pleno disfrute, además de adoptar las medidas legislativas, administrativas y de otra índole que sean necesarias para asegurar el pleno ejercicio de los derechos humanos, entre éstos, los derechos humanos a la libertad de expresión y a defender derechos humanos.

23. De la información obtenida por este Organismo Nacional sobre el caso, así como del análisis de la normatividad sobre intervención de comunicaciones privadas contenidas en la Ley de Seguridad Nacional, en el Código Nacional de Procedimientos Penales y en el Código Militar de Procedimientos Penales, se ha identificado la ausencia de un marco jurídico sobre la adquisición y uso de tecnologías para la intervención de las comunicaciones privadas, con el objeto de recolectar información por parte de instituciones del Estado mexicano, el cual regule su empleo y evite su uso arbitrario, lo anterior, sin perjuicio de la determinación a la que arribe la FEADLE en la investigación que realiza en la CI sobre la presunta intervención ilegal de comunicaciones privadas de las personas relacionadas en dicha indagatoria.

24. Cabe señalar que, en virtud de diversas notas periodísticas publicadas en noviembre de 2019, este Organismo Nacional advirtió que una persona periodista tuvo acceso a través de un tercero a información sobre los registros presuntamente generados por

Pegasus, consistentes en tablas con llamadas, mensajes y correos electrónicos recibidos en el teléfono celular de un ex servidor público mientras se desempeñaba como integrante del Gabinete de Seguridad, indicando que a través de dicho sistema se accedió a listas de contactos de personas servidoras públicas, periodistas, legisladores, colaboradores cercanos, así como de la familia del referido ex funcionario.

25. De igual forma, de acuerdo con la información obtenida por la persona periodista y difundida públicamente en las notas aludidas, se realizaron 46 “ataques” mediante el uso de Pegasus en contra de periodistas, personas defensoras de derechos humanos y activistas, entre el 15 de abril de 2016 y el 7 de junio de 2017, periodo en que una entidad del gobierno federal tenía a su cargo el manejo de Pegasus.

26. Aunado a lo anterior, el 23 de julio de 2021, **O3** publicó un informe en el que se hace referencia a diversos documentos obtenidos por organizaciones de la sociedad civil y medios de comunicación, que acreditan la suscripción de diversos contratos por instituciones del Estado mexicano con **E2** para la adquisición de Pegasus.

27. El documento de referencia incorpora copia de la versión pública de dos contratos obtenidos por **O3** a través de solicitudes de acceso a la información, celebrados por una institución del gobierno federal. El primero de ellos fue realizado el 31 de mayo de 2016, para la adquisición de un sistema con características semejantes al programa Pegasus, y el segundo, fue suscrito el 01 de agosto de 2016, para el servicio y actualización de éste, ambos contratos se llevaron a cabo con **E6.**

28. El informe de referencia también incorpora la investigación periodística en la que se publicaron dos facturas emitidas por **E6**; la primera de ellas de 9 de junio y la segunda de 10 de agosto de 2016, señalando que el monto de la primera factura coincide con el contrato signado entre una entidad del gobierno federal y **E6** para la adquisición del programa Pegasus**.**

29. Dichas pruebas documentales que, en su oportunidad, pudieron ser consideradas como pruebas presuncionales para acreditar indiciariamente la adquisición de Pegasus

por una entidad del gobierno federal, adquieren el carácter de prueba plena ante el comunicado oficial que realizó **A7**, el 07 de mayo de 2020**,** en el que informa que en efecto, esa institución del Estado mexicano adquirió dicho sistema.

30. Lo anterior es de notoria relevancia al considerar que las dos facturas aludidas en la referida investigación periodística fueron libradas a nombre de una entidad centralizada del gobierno federal en 2016.

31. Adicionalmente, la investigación periodística a la que alude el documento de mérito también incorpora información sobre una transferencia de **E6** a **E2**, responsable de Pegasus, y refiere datos sobre el contrato celebrado entre otra institución del gobierno federal y **E5** para la adquisición de Pegasus, así como la renovación de licencia y de contrato durante 2016 y 2017 con **E6** y **E7**, respectivamente.

32. Por otra parte, el informe en mención incorpora además, datos sobre los contratos celebrados entre diversa entidad del Estado mexicano y **E3** para la adquisición de Pegasus, así como respecto a una investigación periodística que identificó una factura emitida en 2016 por **E6** a nombre de dicha entidad pública, bajo el concepto: “Servicio de Monitoreo remoto de Información en el periodo de 1ro al 31 de agosto del 2016”. También proporciona información sobre diversos contratos celebrados entre 2015 y 2018, por esa instancia federal con diversas empresas relacionadas con la venta de Pegasus y transferencia de dinero a **E2**, cuya información se encuentra detallada en el informe aludido.

33. En el mismo tenor, el 28 de julio de 2021, **A7** en conferencia de prensa informó de manera oficial que después de realizar una búsqueda exhaustiva se localizaron 31 contratos otorgados a diversas empresas relacionadas con **E2.**

34. De acuerdo con la información oficial proporcionada por **A7,** se localizaron 16 contratos signados con las empresas **E8** y **E9**, dos contratos suscritos con **E10** y **E11**, siete contratos signados con **E11**, **E12**, **E13** y **E14**, así como dos contratos suscritos con

E11, todos ellos celebrados con diversas entidades del gobierno federal, entre los años 2011 a 2018; información que fue entregada a la Fiscalía General de la República.

35. Cabe mencionar que **A7** publicó en su página oficial la versión pública de 27 contratos, a excepción de los cuatro que refiere fueron signados por **A3,** especificando que dicha autoridad no ha proporcionado los contratos de mérito.

36. Adicionalmente se precisa que de la lectura de las versiones públicas de los 27 contratos difundidos por **A7**, se advierte que varios de éstos corresponden a la adquisición de uniformes, vestuario, botas y calzado, medicamentos, mantenimiento de stand de tiro, adquisición de circuitos cerrados de seguridad perimetral y física de instalaciones, entre otros, y no a la adquisición de sistemas de vigilancia, intervención y recopilación de información similares o análogos a Pegasus**.**

37. No obstante, **A7** informó de manera pública que **E2** utilizó compañías "fachada" a través de las cuales realizó diversos contratos "presuntamente" relacionados con Pegasus y varias instancias del gobierno federal por conceptos distintos al uso de tecnología de inteligencia, y especificó que, en ese tenor, los 31 contratos cuya información difundió, corresponden a empresas vinculadas en sus actividades a **E2**, mismos que fueron signados entre 2011 y 2018; razón por la cual **A7** entregó dicha información a la Fiscalía General de la República para que en ejercicio de sus facultades constitucionales realice la investigación correspondiente.

38. La información antes descrita motiva que este Organismo Nacional haga un llamado urgente a la FEADLE a fin de que investigue de manera exhaustiva en la **CI** los hechos descritos y determine a la brevedad posible, las responsabilidades correspondientes de todos los servidores públicos y terceros involucrados en los hechos.

39. En relación con lo anterior, este Organismo Autónomo subraya que en sus investigaciones la FEADLE no podrá exigir a la persona periodista que accedió a la información descrita en párrafos precedentes, a revelar sus fuentes ni tampoco podrá ser víctima de alguna acusación bajo el argumento de revelar información que pudiera

estar clasificada como reservada y/o confidencial, ya que ello actualizaría en su persona y en la de sus colaboradores una violación inmediata a su derecho a la libertad de expresión.

40. Al respecto, el Relator Especial para la Libertad de Expresión de la CIDH advirtió que:

> […] *la protección del derecho a la reserva de las fuentes periodísticas es clave para la libertad de expresión. Quienes buscan información de interés público pueden ampararse en la reserva de la fuente para poder acceder, buscar e investigar sobre temas de interés público. Muchas de las investigaciones sobre corrupción han sido posibles gracias al acceso a información reservada que alguien entrega a cambio de confidencialidad, debido a que de conocerse su identidad podría sufrir represalias. En "Internet", el acceso a este tipo de información reservada se ha extendido. En estos casos, tiene que quedar claro que el periodista no está cometiendo un acto ilícito y que por tanto, no puede ser responsable por revelar información que el Estado ha declarado confidencial, ni tampoco se le puede pedir que revele la fuente de dicha información*.[9]

41. En tanto que el Principio 8 de la Declaración de Principios sobre la Libertad de Expresión establece que: "*Todo comunicador social tiene derecho a la reserva de sus fuentes de información, apuntes y archivos personales y profesionales*."

42. Sobre dicho Principio, la CIDH ha comentado que el derecho a negarse a revelar las fuentes de información, así como el producto de sus investigaciones se actualiza frente a entidades privadas, terceros, autoridades públicas o judiciales. "*Vale destacar que*

9 *Estándares internacionales de libertad de expresión: Guía básica para operadores de justicia en América Latina*. "*La protección del derecho a la reserva de las fuentes periodísticas es clave para la libertad de expresión.*" 2017; Center for International Media Assistance (CIMA), pág. 39.

dicho derecho no se constituye como deber, ya que el comunicador social no está obligado a guardar el secreto de sus fuentes de información, sino por razones de profesionalismo y de ética profesional".[10]

43. Agrega que: "*Una de las bases primarias del derecho a la reserva se constituye sobre la base de que el periodista, en su labor de brindar información a las personas y satisfacer el derecho de las mismas a recibir información, rinde un servicio público importante al reunir y difundir información que de otra forma, sin guardar el secreto de las fuentes, no podría conocerse. Asimismo, el secreto profesional consiste en guardar discreción sobre la identidad de la fuente para asegurar el derecho a la información; se trata de dar garantías jurídicas que aseguren su anonimato y evitar las posibles represalias que puedan derivar después de haber revelado una información.*"[11]

44. Cabe señalar que la problemática que se aborda en la presente Recomendación General no se refiere solamente a la ejecución de un acto de autoridad que lesiona un derecho subjetivo, el cual en todo caso, es materia de la investigación que realiza la FEADLE, consistente en los intentos de infección con Pegasus a dispositivos móviles de personas periodistas y defensoras de derechos humanos, realizados entre 2015 y 2016, ya que aunado a ello, las circunstancias que inciden en posibles violaciones a derechos humanos derivan de la subsistencia de una situación de hecho, que por sus características peculiares trasciende a los derechos humanos de las personas que se localizan en el territorio mexicano.

45. Este Organismo Nacional advierte que la problemática planteada incide en la posible violación a derechos humanos a la seguridad jurídica, legalidad, libertad de expresión y derecho a defender con carácter colectivo, en virtud de que tales violaciones se actualizan no sólo por los intentos de infección a través de los mensajes maliciosos que las personas periodistas, comunicadoras y defensoras de derechos humanos que presentaron queja ante este Organismo Nacional refirieron haber recibido durante 2015 y 2016, sino por las condiciones que implican un riesgo para todas las personas que se

10 "Antecedentes e Interpretación de la Declaración de Principios". Apartado B. Principio 8, párrafos 36 y 37.
11 *Ídem*.

encuentran en el territorio nacional derivado de la ausencia de normas de carácter general que regulen una problemática específica.

46. Aunado a lo anterior, este Organismo Nacional advierte que, tratándose de personas periodistas y defensoras de derechos humanos, la labor que realizan puede originar una situación de riesgo mayor para el uso de tecnologías para la vigilancia, intervención y recolección de datos, toda vez que las circunstancias derivadas de la generalidad, vaguedad y/o ambigüedad de las normas que establecen los actos que constituyen amenazas a la seguridad nacional e investigación de ciertos delitos, facilita que las autoridades puedan considerar algunas actividades de defensa, denuncia pública, búsqueda y publicación de información realizadas por periodistas y personas defensoras de derechos humanos como actividades “sospechosas”, “subversivas”, “problemáticas” o “riesgosas” para la seguridad nacional.

47. Estas condiciones actualizan e incrementan el riesgo de que las autoridades realicen actos de espionaje en agravio de periodistas y personas defensoras de derechos humanos que excedan los límites legales, mediante el uso de tecnologías cuyo tipo y alcances no se encuentran regulados, bajo el argumento de que estas medidas son necesarias para obtener información que sea útil para “prevenir” cualquier situación que altere el orden público y la paz social.

48. De lo anterior se colige que existe un riesgo real que si bien enfrenta la sociedad misma, es particularmente grave y afecta concretamente la labor de las personas defensoras y periodistas, debido a la alta probabilidad de que se realicen actos de espionaje en su contra bajo los supuestos citados.

49. En ese tenor, esta Comisión Nacional advierte que la sola posibilidad de ser objeto de un ataque a la privacidad genera un efecto amedrentador en el derecho de buscar, recibir y difundir información e ideas de toda índole, así como en las acciones necesarias para ejercer libremente el derecho a defender derechos humanos. En tal virtud, se advierte que las personas periodistas y defensoras de derechos humanos al ejercer tales actividades se encuentran en una situación especial que actualiza el riesgo del posible

uso de tecnologías para el espionaje, intervención y recolección ilegal de datos en su agravio.

50. Con la finalidad de analizar la naturaleza, magnitud y alcances de la problemática planteada que puede incidir en la posible violación a los derechos humanos a la seguridad jurídica, legalidad, libertad de expresión y derecho a defender derechos humanos, es necesario establecer el contexto general en el que se inserta la adquisición y uso de nuevas tecnologías de información y comunicación (TIC's) por los gobiernos.

A. CONTEXTO

51. El desarrollo de nuevas tecnologías de la información y comunicación, así como el uso de éstas motivaron un cambio de paradigma respecto a la utilización de las estructuras tradicionales industriales, a tal grado que el control y manejo de la información ha adquirido un papel preponderante en los procesos socioeconómicos de desarrollo de las naciones, surgiendo lo que ahora conocemos como "Sociedades de la Información".

52. El concepto de "Sociedad de la Información" fue difundido, entre otros autores, por el sociólogo Yoneji Masuda, quien en 1980, la definió como: *"la sociedad que crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad intelectual humana, en lugar del aumento del consumo material"*[12]. En 1998, el sociólogo y economista Manuel Castells señaló que las Sociedades de la Información constituyen un nuevo sistema económico, tecnológico y social, en el que la economía no depende del incremento de los factores de producción, sino en la aplicación del conocimiento y la información"[13].

53. En la actualidad, el uso de las tecnologías de la información y comunicación, como son: internet, los teléfonos inteligentes, los dispositivos con acceso a Wi-Fi, por mencionar algunos, forman parte de la vida cotidiana e impulsan el libre ejercicio de la

12 *La sociedad informatizada como sociedad post industrial*, editorial Fundesco-Tecnos. Madrid, España. 1984.
13 *La era de la información: economía, sociedad y cultura*, editorial Alianza. Madrid, España. 2000.p. 506.

libertad de expresión. Estas tecnologías fomentan la participación democrática de la ciudadanía y propician, de esta manera, la cohesión social, la buena gobernanza y el estado de derecho. Esto se reconoce en el Compromiso de Túnez, adoptado por la *Cumbre Mundial de la Sociedad de la Información*, en la sesión del 15 y 16 de noviembre de 2005, cuya celebración fue aprobada mediante la resolución 56/183 de la Asamblea General de la Organización de las Naciones Unidas[14].

54. Estas tecnologías de la información y comunicación adquieren una dimensión específica al ser utilizadas por personas defensoras de derechos humanos y periodistas, ya que constituyen herramientas imprescindibles de su labor, puesto que, a través de éstas, documentan y denuncian violaciones a derechos humanos, además de coordinar las acciones necesarias para hacerles frente. Los teléfonos celulares, por ejemplo, se utilizan con mucha frecuencia para enviar acciones urgentes y alertas.

55. El uso de estas tecnologías de la información y comunicación permite a las personas defensoras, periodistas, comunicadores y a la ciudadanía en general, salvar los obstáculos que hasta hace algunas décadas implicaba utilizar los sistemas tradicionales de comunicación. En este nuevo paradigma, global y transformador, se amplía el acceso e intercambio de información, surge la posibilidad de emplear páginas web, foros en internet, *blogs*, redes sociales, entre otros, además de poder hacer públicos contenidos propios. Se transforman en medios de defensa social, de denuncia pública, de participación ciudadana, de rendición de cuentas y transparencia, de las entidades y dependencias públicas; de fortalecimiento de la democracia.

56. Este cambio de paradigma en el cual las nuevas tecnologías posibilitan el acceso e intercambio de grandes flujos de información, ha propiciado que los gobiernos busquen nuevas alternativas y mecanismos para realizar acciones de espionaje, con el argumento de “asegurar” el respeto al estado de derecho, particularmente en aspectos vinculados con la seguridad nacional y la investigación de delitos graves, sin embargo, tales medidas

14 Cumbre Mundial de la Sociedad de la Información, Ginebra 2003-Túnez 2005; Compromiso de Túnez, publicado el 28 de junio de 2006. párr. 15.

limitan de manera sensible ciertos derechos humanos, entre ellos la privacidad, impactando a su vez en otros derechos.

57. El Juez de la Corte Interamericana de Derechos Humanos Eugenio Raúl Zaffaroni, y el abogado Guido Leonardo Croxatto, señalan que la privacidad "se refiere, en concreto, a la intimidad de las personas. A su esfera más íntima y personal: allí donde se desarrolla la 'persona'. Sin intimidad, no hay personalidad. No hay conciencia subjetiva. No hay sujeto. No hay identidad. No hay persona."[15]

58. Como un ejemplo de las nuevas alternativas y mecanismos para realizar acciones de vigilancia por parte de los gobiernos podemos mencionar el caso de la Ley Patriota, aprobada por el Congreso norteamericano después de los atentados terroristas del 11 de septiembre de 2001, al amparo de la cual la *National Security Agency* (NSA) podría realizar actividades de escucha masivas mediante el uso de un programa de espionaje, que fue declarado intrusivo por una Corte norteamericana. Sobre este caso, los autores Zaffaroni y Croxatto refieren lo siguiente:

> *"Un tribunal norteamericano declaró ilegal el programa de escuchas de la NSA. La Corte de Apelaciones de la Segunda Sección con sede en Nueva York, falló (el 6 de julio de 2015) contra el programa de espionaje de la NSA en respuesta a una demanda presentada por la Unión Americana de Libertades Civiles (ACLU), entendiendo que las actividades de escuchas ilegales masivas de la NSA alrededor del mundo "exceden lo que el Congreso Americano autorizó" (al aprobar la llamada Ley Patriota, en especial la sección 215 de tal ley, que autoriza al FBI a mantener "registros" con información recopilada alrededor del mundo, incluso en información relativa a "negocios"). Este fallo (que declaraba ilegal el programa de espionaje masivo llevado adelante por la NSA, que se amparaba en una ley que había sido aprobada en EEUU*

15 "El espionaje masivo como un (nuevo) crimen de agresión", en *Pensar en Derecho*, UBA; Buenos Aires, diciembre de 2015, p. 341.

tras los atentados terroristas del 11 de septiembre de 2001), luego sería rectificado por otro tribunal superior, alegando que los demandantes no habían logrado probar durante el proceso "su calidad de víctimas". 16

59. Desde el año 2013, el Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) observó, con motivo de la información sobre la existencia y alcance de los programas de vigilancia que fue revelada a partir de documentos proporcionados a la prensa por Edward Snowden,[17] que se ha generado un amplio debate sobre el alcance y los controles de dichos programas, debido a que operan bajo reglas de reserva y confidencialidad y se encuentran, en su mayoría, sometidos a controles de comités especiales[18].

60. La información revelada por Edward Snowden generó una profunda crisis que afectó, según Zaffaroni, "*no solo la legitimidad de los Estados democráticos modernos (la base misma de lo que entendemos por Estado de Derecho, por democracia, por sociedad civil) que tiene como una de sus misiones centrales preservar las garantías civiles (siendo la privacidad de las comunicaciones – garantía de autonomía personal, libertad de expresión- una de ellas, una de las más fundamentales en una democracia), sino también la efectividad y sentido mismo de la diplomacia, de los espacios internacionales públicos, de los foros donde se negocia –en principio- de buena fe y donde se busca, generen y consoliden acuerdos (el escándalo del espionaje masivo a dirigentes, políticos, embajadores, jueces, estudiantes, empresarios, etc.)*".[19]

61. De igual forma, el Relator Especial para la Libertad de Expresión de la CIDH señaló que estas revelaciones ponen en evidencia los riesgos a la libertad de pensamiento y

16 *Ibidem*, pp. 339 y 340.

17 Edward Joseph Snowden (Elizabeth City, Carolina del Norte; 21 de junio de 19831) es un consultor tecnológico estadounidense, informante, antiguo empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA), que en junio de 2013, a través de los periódicos The Guardian y The Washington Post, hizo públicos documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore.

18 CIDH. Informe Anual de la Relatoría Especial para la Libertad de Expresión 2013. párr. 394.

19 E. R. Zaffaroni y G. L. Croxatto, *Op. Cit*., pp. 355 y 356.

expresión de las nuevas tecnologías y técnicas de vigilancia, así como "*la necesidad de revisar la legislación correspondiente y de establecer mayores mecanismos de transparencia y control, de conformidad con el derecho internacional de los derechos humanos*"[20].

62. Así mismo, el Relator Especial para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión de las Naciones Unidas y la entonces Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión, instaron a las autoridades a revisar la legislación respectiva y modificar sus prácticas con la finalidad de asegurar su adecuación a los principios internacionales.[21]

63. En consecuencia, este Organismo Nacional reconoce que, en un entorno en el cual hay un flujo constante de información a través de dispositivos inteligentes, las actividades de vigilancia, intervención y recopilación de datos a cargo del Estado mexicano pueden tener múltiples efectos negativos para el ejercicio y goce de los derechos humanos, particularmente cuando tales acciones se dirigen a personas que ejercen labores de información, defensa y protección de derechos fundamentales.

64. Lo anterior en virtud de que la sola amenaza de ser objeto de actos de vigilancia puede producir en la persona efectos semejantes a los que se generan ante la certeza de encontrarse vigilado, siendo la autocensura uno de los más graves.[22] Esta circunstancia lesiona profundamente el tejido social cuando la padecen periodistas, comunicadores y personas defensoras de derechos humanos.

65. Resulta necesario identificar de manera clara en qué momentos y bajo qué hipótesis normativas las actividades de vigilancia, intervención y recopilación de datos desarrolladas por los gobiernos son actividades lícitas, con un objetivo legítimo, para

20 CIDH, *Op. Cit*. 2013, párr. 395.
21 Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión, publicada el 21 de junio de 2013.
22 Zaffaroni y Croxatto, *Op. Cit*., p. 346.

determinar, en oposición a ello, cuándo pueden constituir espionaje, actos arbitrarios, ilegales y conculcatorios de derechos humanos, en perjuicio no sólo de las personas a quienes se dirigen tales acciones sino de la sociedad misma.

66. Parte del origen del discurso para justificar el uso de estas tecnologías, tiene que ver con la manifestación de los gobiernos respecto a que en el cumplimiento de su obligación de garantizar a las personas el ejercicio libre de sus derechos, han adoptado diversas medidas para prevenir y contrarrestar el terrorismo, incluyendo la vigilancia electrónica y el uso de mecanismos de seguimiento, además de ampliar significativamente las facultades de vigilancia en los últimos años.[23] Esta "lucha contra el terror" o "guerra contra el terrorismo" ha sido la razón alegada por numerosos gobiernos para legitimar, además de "endurecer", las medidas de vigilancia, intervención y recolección de datos mediante el uso de nuevas tecnologías, argumentando que es necesario el uso de tales métodos para la investigación de conductas lesivas a la seguridad, orden y paz social, tipificadas como delitos.

67. En el caso de México, el discurso "legitimador" de la adquisición y uso de dichas tecnologías encuentra sustento en la "prevención, disuasión, contención y desactivación de amenazas y riesgos que pongan en peligro los bienes jurídicos que tutela la Seguridad Nacional (población, territorio, instituciones de gobierno, soberanía, orden constitucional y la democracia para el desarrollo)", y la "investigación de conductas lesivas a la seguridad, orden y paz social".

68. Esta Comisión Nacional cuenta con información de la cual se advierte que diversas entidades públicas del Estado mexicano adquirieron Pegasus entre los años 2011 a 2017, así como otros programas para la intervención de comunicaciones privadas. Aunque no hay estudios sobre la potencialidad lesiva de otros sistemas semejantes a Pegasus, no significa que representan un riesgo menor, ya que también son intrusivos y respecto de ellos; al igual que en el caso de Pegasus, no se proporcionó información a este Organismo Nacional sobre si su elección atendió a criterios específicos sobre su

23 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. "Los Derechos Humanos, el terrorismo y la lucha contra el terrorismo." Folleto No. 32. pp. 48 y 49.

capacidad para captar información, ni se proporcionaron estudios o análisis adecuados para su adquisición que abordaran su capacidad lesiva. Tampoco se informó a este Organismo Nacional si hay restricciones de uso solicitadas o previstas en los contratos respectivos, salvaguardas a derechos humanos, ni que se prevea la responsabilidad de las empresas desarrolladoras y/o distribuidoras de tales sistemas en el caso de que el uso de esas tecnologías ocasione violaciones a derechos humanos.

69. En virtud de la reserva de información prevista en los artículos 4, párrafo segundo; 113 fracciones I y V, de la Ley General de Transparencia y Acceso a la Información Pública; 3, 110 fracciones I y V, de la Ley Federal de Transparencia y Acceso a la Información Pública, en los lineamentos Décimo Séptimo y Vigésimo Sexto, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas[24], y en relación con lo dispuesto en los numerales 51 y 54 de la Ley de Seguridad Nacional, este Organismo Nacional se encuentra impedido por disposición legal expresa para hacer pública la información concerniente a datos de personas físicas que participaron en la contratación y/o tienen conocimiento de los métodos y especificaciones técnicas de sistemas adquiridos para la intervención de comunicaciones privadas, pues su divulgación permitiría su identificación y localización, lo que podría propiciar riesgos para su vida y seguridad. Asimismo, se encuentra impedido para difundir información respecto a especificaciones técnicas y métodos de operatividad de tales sistemas, ya que su divulgación podría potencializar un riesgo o amenaza a la Seguridad Nacional, al tratarse de datos que pudieran ser útiles para la generación de contra inteligencia.

70. Además, acorde con lo establecido en los artículos: 113 fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 3, 110 fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, lineamento Vigésimo Tercero de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en relación con lo previsto en el artículo 218 del Código Nacional de Procedimientos Penales, este

24 Publicados en el Diario Oficial de la Federación, el 15 de abril de 2016.

Organismo Autónomo se encuentra impedido para difundir información específica obtenida, en virtud de la consulta realizada a la CI a cargo de la FEADLE, toda vez que a la fecha del presente pronunciamiento dicha indagatoria se encuentra en integración y la divulgación de información sensible que obre en ésta podría obstruir la adecuada investigación de delitos.

71. En el mismo tenor, este Organismo Nacional se encuentra impedido por disposición legal expresa, para hacer pública la información que le fue proporcionada con ese carácter por las entidades que adquirieron tecnologías para la vigilancia, intervención y recolección de datos, lo anterior en virtud de que la información clasificada de origen por otra autoridad únicamente puede ser desclasificada por el sujeto obligado que realizó tal clasificación, acorde a lo establecido en el Título Cuarto, Capítulo I, de la Ley Federal de Trasparencia y Acceso a la Información Pública, así como Capítulo IV de los citados Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, por lo que este Organismo Nacional no se encuentra facultado para proporcionar la información que le fue entregada con tal carácter.

72. Ello sin embargo, no impide que esta Comisión Nacional advierta el grave riesgo de la posible ejecución de violaciones a los derechos humanos a la seguridad jurídica y legalidad, atendiendo a la subsistencia de marcos regulatorios deficientes relativos a la intervención de comunicaciones, así como a las facultades discrecionales de los órganos de inteligencia y de las autoridades de procuración de justicia para realizar actos de vigilancia mediante el uso de cualquier clase de tecnología.

73. Tampoco impide que se advierta la posibilidad de que se actualicen violaciones a los derechos humanos a la libertad de expresión y al derecho a defender, ya que la ausencia de mecanismos y controles efectivos por órganos independientes, así como la falta de una regulación sobre el tipo y alcances de tecnologías que pueden ser adquiridas y utilizadas en la intervención de comunicaciones, crea condiciones propicias para que su uso pueda rebasar los fines constitucionalmente permitidos.

74. Lo anterior es así, ya que tales tecnologías pueden ser empleadas bajo esquemas legales que no corresponden a su potencialidad lesiva creando con ello un riesgo grave, que por su sola existencia genera un efecto amedrentador que impacta de manera particular a las personas defensoras de derechos humanos y periodistas, dado que dicho riesgo puede generar autocensura e inhibir así la labor que realizan, con lo que también se actualiza un riesgo sobre el pleno ejercicio de los derechos humanos señalados.

75. Esta Comisión Nacional afirma lo anterior, ya que como se expuso en párrafos precedentes, se encuentra plenamente acreditado que entidades públicas del Estado mexicano efectivamente adquirieron Pegasus entre los años 2011 a 2017, así como diversos sistemas desarrollados para fines semejantes, y aunque corresponde a la FEADLE determinar si dicho sistema o alguno semejante ha sido utilizado en contra de personas periodistas, defensoras de derechos humanos, o de alguna otra persona en territorio nacional con motivo de la integración de la **CI**, es relevante destacar el grave riesgo de violaciones a los derechos humanos ante la subsistencia de las siguientes circunstancias:

- Autoridades del gobierno federal adquirieron Pegasus en el periodo de 2011 a 2017, cuya potencialidad lesiva ha sido objeto de estudio por la organización **O1**.

- Otras entidades públicas han adquirido tecnologías para la vigilancia, intervención y recolección de datos.

- Entre 2015 y 2016 personas periodistas y defensoras de derechos humanos recibieron mensajes de texto maliciosos en sus teléfonos móviles, los cuales se identificaron como intentos de infección a través de Pegasus en el estudio realizado por **O1.**

- Las fechas en que las personas periodistas y defensoras de derechos humanos refieren haber recibido tales mensajes durante 2015 y 2016, coinciden con el periodo en el cual se acreditó que Pegasus efectivamente fue adquirido por instituciones del gobierno mexicano.

- No hay regulación específica sobre el uso, alcances y límites de tales tecnologías.

- El marco regulatorio actual sobre intervención de comunicaciones privadas otorga a los órganos de inteligencia y de procuración de justicia facultades discrecionales.[25]

76. Con ello se genera un riesgo, el cual constituye una situación de hecho que debe ser urgentemente atendida por el Estado mexicano, ya que su subsistencia incide en la posibilidad de que se violen derechos humanos y con ello que el Estado mexicano incumpla con el deber de cuidado que emana del derecho humano a la seguridad jurídica, al tenor de los razonamientos que se exponen en los siguientes apartados**.**

B. MARCOS REGULATORIOS DEFICIENTES SOBRE LA INTERVENCIÓN DE COMUNICACIONES PRIVADAS

77. Este Organismo Nacional ha identificado los siguientes aspectos del actual marco regulatorio como elementos que constituyen deficiencias que podrían derivar en violaciones a los derechos humanos señalados en el texto de la presente Recomendación General:

B.1. Deficiencia por normas que conceden facultades discrecionales a órganos de inteligencia y autoridades de procuración de justicia para realizar actos de vigilancia mediante el uso de cualquier tecnología

78. El derecho a la seguridad jurídica está garantizado en el sistema jurídico mexicano a través de los artículos 14 y 16 de la Constitución Política de los Estados Unidos Mexicanos, que prevén el cumplimiento de las formalidades esenciales del procedimiento, la autoridad competente, así como la fundamentación y motivación de la causa legal del procedimiento.

25 Suprema Corte de Justicia de la Nación, Registro digital: 328714, Instancia: Segunda Sala, Quinta Época, Materias(s): Común, *Semanario Judicial de la Federación*, tomo LXVI, pág. 1599, Tipo: Aislada, AUTORIDADES, FACULTAD DISCRECIONAL DE LAS.

79. Las obligaciones de las autoridades del Estado mexicano para cumplir con el derecho a la certeza jurídica y legalidad están previstas también en los artículos 8 y 10 de la Declaración Universal de Derechos Humanos; 14 del Pacto Internacional de Derechos Civiles y Políticos; 8 y 25 de la Convención Americana sobre Derechos Humanos; XXVI, párrafo segundo, de la Declaración Americana de los Derechos y Deberes del Hombre, así como en la Resolución de la CrIDH en el Caso Kawas Fernández vs Honduras, en los que se reconoce que se debe garantizar a las personas el derecho, en condiciones de plena igualdad, a ser oídas públicamente y con justicia por un tribunal independiente e imparcial, para la determinación de sus derechos y obligaciones o para el examen de cualquier acusación en su contra.

80. El derecho a la seguridad jurídica comprende el principio de legalidad, al establecer que los poderes públicos deben estar sujetos al derecho bajo un sistema jurídico coherente y permanente, dotado de certeza y estabilidad que especifique los límites del Estado en sus diferentes esferas de ejercicio en atención a los titulares de los derechos individuales, garantizando el respeto a los derechos fundamentales de las personas.

81. Para cumplir o desempeñar sus obligaciones, los agentes del Estado deben cubrir todos los requisitos, condiciones y elementos que exige la Constitución Política de los Estados Unidos Mexicanos y demás leyes que de ella emanan, así como los previstos en los instrumentos internacionales suscritos y ratificados por el Estado mexicano, para que la afectación en la esfera jurídica de los particulares que en su caso genere, sea jurídicamente válida, ya que el acto de autoridad debe estar debidamente fundado y motivado. Así, la restricción de un derecho debe ser utilizada estrictamente para los casos que lo ameriten, a fin de garantizar el derecho a la seguridad jurídica de los gobernados.[26]

82. El derecho a la seguridad jurídica también constituye un límite a la actividad estatal como el conjunto de requisitos que deben observarse en todas las instancias a efecto de

26 CNDH, Recomendaciones: 35/2017, párr. 89; 71/2016 párr. 44; 70/2016, de 29 de diciembre de 2016, párr. 110; 69/2016 párr. 50; 60/2016 párr. 95; 39/2016 párr. 38; 37/2016 párr. 68 y 58/2015 párr. 220, entre otras.

que las personas estén en condiciones de defender adecuadamente sus derechos ante cualquier acto de la autoridad que pueda afectarlos.[27]

83. Es menester precisar que un acto de autoridad puede ser conculcatorio de los derechos humanos de seguridad jurídica y legalidad a pesar de encontrarse fundado y motivado en una norma, si ésta última establece facultades discrecionales que en condiciones específicas pueden ser ejercidas de manera arbitraria por la autoridad.[28]

84. Es necesario distinguir entre el acto de autoridad reglado, el acto de autoridad discrecional y el acto de autoridad arbitrario. De acuerdo con un sector doctrinario el primero de ellos es aquél en que la actividad administrativa de la autoridad se encuentra determinada tanto en su momento, como en su contenido y forma. La norma jurídica especifica la conducta administrativa y limita su arbitrio o libertad, no deja margen alguno para la apreciación subjetiva del agente sobre la circunstancia del acto.[29]

85. El acto de autoridad discrecional es aquél en que la norma deja a la administración un poder de libre de apreciación para decidir si debe actuar o abstenerse, en qué momento debe actuar, cómo debe hacerlo o qué contenido debe dar a su actuación. En este tipo de actos, la ley dota a la autoridad la libertad de decidir su actuación bajo criterios de conveniencia, necesidad, equidad, razonabilidad, suficiencia, exigencia de interés u orden público. Estos actos discrecionales siempre deben atender al principio de interés público y al principio de legalidad.[30]

86. El acto arbitrario es aquél que habiendo sido establecido en la norma como discrecional, es efectuado sin realizar un proceso de razonabilidad, investigación, verificación y deja de atender los principios de interés público y de legalidad.[31]

---

27 CNDH Recomendaciones: 35/2017, párr. 90; 22/2017 párr. 110; 71/2016 párr. 42; 70/2016 párr. 109; 69/2016 párr. 46 donde se invoca el *Caso Fermín Ramírez vs. Guatemala*, sentencia de 20 de junio de 2005, párr. 110. Voto razonado del juez Sergio García Ramírez, de 18 de junio de 2005.
28 Tribunales Colegiados de Circuito, Tesis administrativa. "Facultades discrecionales de la administración. Los administrados tienen interés jurídico para impugnar su ejercicio cuando afecten sus derechos." *Semanario Judicial de la Federación*, diciembre de 2012, registro 2002304.
29 José Humberto Sánchez Gutiérrez, *Acto Discrecional. Principios que lo rigen y su jerarquía*. UNAM. México, p. 349.
30 *Ibid*., pp. 350 y 351.
31 *Ibid*., pág. 354.

87. En México la intervención de comunicaciones[32] se encuentra prevista en el artículo 16, párrafos12, 13 y 15, de la Constitución Política de los Estados Unidos Mexicanos[33], precepto que establece como requisito *sine qua non* la expedición de una orden judicial que autorice expresamente la ejecución de dicha medida a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público local o federal, con excepción de casos electorales, fiscales, mercantiles civiles, laborales o administrativos, o bien tratándose de las comunicaciones entre el detenido y su defensor.

88. De acuerdo con el texto constitucional, la facultad para solicitar al Poder Judicial de la Federación la autorización para la intervención de comunicaciones privadas se encuentra regulada por normas secundarias, que precisan qué autoridades tienen competencia para realizar tales solicitudes, así como las hipótesis normativas de su procedencia.

89. Del análisis del marco normativo nacional se advierte que la intervención de comunicaciones es una medida que exclusivamente se prevé bajo dos hipótesis de procedencia: la primera de ellas, para la investigación de amenazas a la seguridad nacional según lo prevé la Ley de Seguridad Nacional, y la segunda, para la investigación de delitos, tanto en el fuero civil como en asuntos de jurisdicción militar, de acuerdo a lo establecido de manera general en el Código Nacional de Procedimientos Penales y en

32 Cabe señalar que si bien el texto constitucional hace referencia a las "comunicaciones", el espionaje, intervención y recopilación de datos a través de sistemas con la capacidad de Pegasus**,** no se limitan exclusivamente a la intervención de comunicaciones como son las llamadas telefónicas o mensajes de texto vía redes sociales, sino que involucran la posibilidad de realizar "escuchas" y grabaciones a través de los micrófonos y cámaras con que cuentan los dispositivos electrónicos, con lo cual existe además el riesgo de limitación y afectación al derecho humano a la privacidad, que a su vez incide de manera directa en el ejercicio de los derechos humanos de libertad de expresión, reunión y asociación, así como el derecho a defender derechos humanos.

33 Artículo 16. […] "*Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley*.
Exclusivamente la autoridad judicial federal, a petición de la autoridad federal, que faculte la ley, o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.
[…]
Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con estos carecerán de todo valor probatorio".

el Código Militar de Procedimientos Penales, respectivamente, sin perjuicio de su mención en otras normas adjetivas y reglamentarias.

90. En el sistema tradicional de justicia penal, la intervención de comunicaciones procede cuando hay indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves. Sin embargo, en el actual sistema acusatorio se establece que tal medida podrá realizarse "cuando se considere necesario en la investigación"[34], con lo cual se abre la posibilidad de que en ejercicio de dicha facultad discrecional se omita realizar este análisis sobre racionalidad y verificación que asegure la legalidad y pertinencia de la medida.

91. Respecto a la primera hipótesis legal de procedencia, se advierte que la Ley de Seguridad Nacional establece que la intervención de comunicaciones implica la toma, escucha, monitoreo, grabación o registro de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología. De acuerdo con la ley en cita, la intervención de comunicaciones privadas procederá cuando se emplee para la investigación de amenazas a la seguridad nacional, conforme a las hipótesis normativas establecidas en el artículo 5 de la referida ley, en cuyo caso el gobierno mexicano puede hacer uso de "*los recursos que legalmente se encuentren a su alcance*", inclusive de información anónima. El Centro realizará la solicitud de autorización al Poder Judicial de la Federación y llevará a cabo el control y la ejecución de la orden respectiva.[35]

92. Así mismo, la Ley de Seguridad Nacional prevé que la solicitud debe contener *"una descripción detallada de los hechos y situaciones que representen alguna amenaza para la seguridad nacional en los términos del artículo 5"*, así como *"las consideraciones que motivaron la solicitud"* y *"el lapso de vigencia de la autorización que se solicita"*.[36]

93. El juez federal emitirá la resolución correspondiente en un plazo de veinticuatro horas contadas a partir de la recepción de la solicitud. En caso de autorizarla, debe precisar

34 Código Federal de Procedimientos Penales: Artículo 278 Ter. Código Nacional de Procedimientos Penales: Artículo 291.
35 Ley de Seguridad Nacional. Artículos 5, 33, 34, párrafo segundo, 35 y 41, párrafo primero.
36 *Ibidem*. Artículo. 38.

los datos de identificación del expediente en que se actúa; el tipo de actividad que autoriza; el lapso durante el cual se autoriza la medida y, en caso necesario, la autorización expresa para instalar o remover cualquier instrumento o medio de intervención, así como cualquier otra apreciación que el Juez considere pertinente.[37]

94. En este contexto, el juez federal autorizará la intervención de comunicaciones privadas por un periodo máximo de ciento ochenta días naturales y, en casos de excepción debidamente justificados, podrá autorizar una prórroga hasta por un periodo igual al original; la solicitud de prórroga se realizará con las mismas formalidades, señalando las razones por las cuales continúa siendo necesaria la intervención de comunicaciones para investigar una amenaza de seguridad nacional.[38]

95. No obstante, la ley en cita también establece lo siguiente: "*cuando el cumplimiento del procedimiento establecido en la Sección II del presente Capítulo comprometa el éxito de una investigación y existan indicios de que pueda consumarse una amenaza a la Seguridad Nacional, el juez, por la urgencia, podrá autorizar de inmediato la medida que se requiera"*[39], lo que nuevamente implica la posibilidad de que tal medida sea autorizada sin el análisis acucioso previo que asegure su legalidad y pertinencia.

96. La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha sostenido que la intervención de comunicaciones para investigar amenazas a la seguridad nacional a cargo de sistemas o entidades de inteligencia es permitida, ya que su finalidad es proteger un interés jurídico relevante y necesario para la sociedad. Este órgano señaló que "*la vigilancia legal y dirigida de la comunicación digital puede constituir una medida necesaria y efectiva para la inteligencia que llevan a cabo las entidades encargadas de hacer cumplir la ley de conformidad con las normas internacionales y nacionales. Vigilancia por razones de seguridad nacional o por la prevención del terrorismo u otro delito puede ser un 'objetivo legítimo'."*[40]

37 *Ibid*. Artículos 39 y 40.
38 *Ibid*. Artículos 43 y 44.
39 *Ibid*. Artículo 49.
40 Informe: El Derecho a la privacidad en la era digital. A/HCR/ 27/37.30 de junio de 2014. Párr. 24.

97. No basta, sin embargo, que una ley prevea de manera general la intervención de comunicaciones privadas para que se considere que no es arbitraria e ilegal, sino que deberá acreditarse que hay un objetivo legítimo y que la aplicación de esta medida es proporcional, necesaria e idónea.

98. Lo anterior es así, porque la intervención de comunicaciones como medio de vigilancia, intervención y recopilación de datos, aun cuando se realice en atención a un "objetivo legítimo", limita el derecho humano a la privacidad, tutelado en los artículos 12 de la Declaración Universal de Derechos Humanos; 11 de la Convención Americana sobre Derechos Humanos; 17 del Pacto Internacional de Derechos Civiles y Políticos; 5 de la Declaración Americana de los Derechos y Deberes del Hombre; 14 de la Convención Internacional sobre la Protección de los derechos de los trabajadores migratorios y sus familiares, y 16 de la Convención sobre los Derechos del Niño de las Naciones Unidas; así como en la Declaración de Principios sobre la Libertad de Expresión, y en los Principios de Johannesburgo sobre Seguridad Nacional, Expresión y Acceso a la Información.[41]

---

41 Declaración Universal de Derechos Humanos. Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Convención Americana de Derechos Humanos. Artículo 11. Protección de la Honra y de la Dignidad. 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie 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. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Pacto Internacional de Derechos Civiles y Políticos. Artículo 17. 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Declaración Americana de los Derechos y Deberes del Hombre. Artículo 5. Derecho a la protección a la honra, la reputación personal y la vida privada y familiar Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

Convención Internacional sobre la Protección de los derechos de los trabajadores migratorios y sus familiares. Artículo 14. Ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques.

Convención sobre los Derechos del Niño de las Naciones Unidas. Artículo 16. 1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

99. La limitación al derecho a la privacidad, a su vez, incide de manera directa en el ejercicio de los derechos humanos de libertad de expresión, reunión y asociación, así como el derecho a defender derechos humanos. Por esto mismo, corresponde al Estado acreditar que las limitaciones impuestas a estos derechos humanos, en virtud de la intervención de comunicaciones privadas, tienen un objetivo legítimo.

100. El contenido y alcance de los principios enunciados también constan en el documento titulado Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, de mayo de 2014, desarrollados por diversos grupos de la sociedad civil en colaboración con expertos internacionales y parte del sector empresarial[42], cuya versión preliminar fue presentada en el Consejo de Derechos Humanos de las Naciones Unidas, en septiembre de 2013, publicándose la versión final en mayo de 2014.[43]

101. En este documento se destaca la necesidad de proteger, no solamente el contenido de las comunicaciones directas, sino también los "metadatos"[44] e información derivada de tales comunicaciones, ya que pueden revelar información sensible como la identidad de una persona, comportamiento, asociaciones, condiciones físicas, médicas, de raza, orientación sexual, nacionalidad, puntos de vista, o bien, permitir el mapeo de la ubicación de la persona, e inclusive de todas aquéllas que se encuentren en un lugar

42 Las organizaciones que participaron fueron: Access, Artículo 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society (India), Comisión Colombiana de Juristas, Electronic Frontier Foundation, European Digital Rights, Fundación Karisma, Open Net Korea, Open Rights Group, Privacy International, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, entre otras. Rodriguez, Katitzia. Thirteen Principles Against Unchecked Survillance Launched at United Nations. *Confr.*: https://www.eff.org

43 Conforme a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, se entenderá por **objetivo legítimo** el que la intervención de comunicaciones tenga por finalidad proteger un interés jurídico predominante, trascendente y necesario para una sociedad democrática, como es el caso de la existencia de amenazas a la seguridad nacional o acciones relativas a la procuración de justicia. La **proporcionalidad** se traduce en que al efectuar un acto de vigilancia a través de la intervención de comunicaciones se debe considerar la sensibilidad de la información a la que se accede, realizando la ponderación de los derechos humanos que pudieren entrar en conflicto con la ejecución de dicha acción. La **necesidad** se refiere a que la intervención de comunicaciones sólo se realice cuando sea el único medio para alcanzar un objetivo legítimo, o bien, cuando existiendo varias alternativas, sea la menos lesiva para los derechos humanos de las personas. La **idoneidad o adecuación** de la intervención de comunicaciones se refiere a que ésta se encuentre autorizada por la ley para cumplir con el objetivo legítimo.

44 Información sobre los datos específicos como identificación del número, fecha, duración de la comunicación y/o localización de la llamada.

determinado, como puede ser el caso de una manifestación o un evento público o privado.

102. El Tribunal de Justicia de la Unión Europea en la sentencia del caso *Digital Rights Ireland y Seitlinger y otros*, estableció que el análisis de los metadatos en su conjunto permite obtener información precisa sobre la vida privada de las personas. Con lo que se puso en evidencia que, contrario a los criterios que sostenían que únicamente había afectación al derecho humano a la privacidad cuando se interceptaba y recopilaba información del contenido de una comunicación directa, también hay una injerencia a la privacidad por la obtención y conservación de los denominados metadatos.[45]

103. Por ende, tanto la información que constituya el contenido de la comunicación, como los metadatos que se originan a partir de ésta, deben ser protegidos con la misma rigurosidad. El Estado tiene la obligación de acreditar en todos los casos que se empleen tecnologías para la vigilancia, intervención y recopilación de datos, que hay un objetivo legítimo, proporcional, necesario e idóneo, puesto que son actos de injerencia a la vida privada.

104. Esto adquiere especial relevancia al considerar que la Ley de Seguridad Nacional no especifica si las formalidades previstas en el Capítulo II, denominado "De las intervenciones de comunicaciones", son aplicables exclusivamente cuando dicha intervención tiene como objetivo el contenido de las comunicaciones y no cuando se interceptan y recopilan metadatos. Aunque el Poder Judicial de la Federación ha emitido criterios específicos al respecto, dichos criterios deben estar incorporados en el texto de la ley para dar mayor claridad y certeza jurídica.[46]

45 8 de abril de 2014; párr. 26, 27 y 37.
46 SCJN; Segunda Sala, Tesis constitucional y penal. "*Comunicaciones privadas. La solicitud de acceso a los datos de tráfico retenidos por los concesionarios, que refiere el artículo 190, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión, debe realizarse en términos del artículo 16 constitucional y sólo la autoridad judicial podrá autorizar la entrega de la información resguardada*". *SEMANARIO JUDICIAL DE LA FEDERACIÓN*, julio de 2016, registro 2011994.
-----; Primera Sala, Tesis constitucional. "*Derecho a la inviolabilidad de las comunicaciones privadas. Su objeto de protección incluye los datos que identifican la comunicación*". *SEMANARIO JUDICIAL DE LA FEDERACIÓN*, agosto de 2011, registro 161335.

105. Los estándares internacionales citados en el cuerpo de la presente Recomendación General son claros al establecer que hay una injerencia en la vida privada, cuando se realizan actos de vigilancia, intervención y recopilación de datos mediante el empleo de tecnologías, ya sea del contenido de comunicaciones, como de los metadatos originados por éstas.

106. En consecuencia, este Organismo Constitucional considera que las intervenciones de comunicaciones que pudiera llegar a realizar el Centro, así como las diversas instituciones de investigación y procuración de justicia, en ejercicio de las facultades que les son conferidas en la Ley de Seguridad Nacional y en el Código Nacional de Procedimientos Penales, respectivamente, podrían llegar a ser "ilegales y arbitrarias" en clara contravención al Pacto Internacional de Derechos Civiles y Políticos, en atención a este manejo discrecional a cargo del órgano de inteligencia y de las instituciones investigadoras de delitos sobre las solicitudes, ejecución y control de tal medida, con lo cual los principios de proporcionalidad, necesidad e idoneidad respecto al objetivo legítimo que es la investigación de amenazas a la seguridad nacional, pudieran no ser satisfechos.

107. México se adhirió al referido Pacto Internacional, el 23 de marzo de 1981, por lo que las disposiciones previstas en éste forman parte de su orden normativo interno y son de obligatoria observancia por todas las autoridades, tanto administrativas como judiciales, de acuerdo con el artículo 1º de la Constitución Política de los Estados Unidos Mexicanos, así como al criterio sustentado por el Pleno de la Suprema Corte de Justicia de la Nación en la contradicción de Tesis 293/2011.[47]

108. El Comité de Derechos Humanos de las Naciones Unidas, en la Observación General 16 "Derecho a la intimidad", reconoció que "*la injerencia autorizada por los Estados sólo puede tener lugar en virtud de una ley, que a su vez debe conformarse a*

47 SCJN, Registro digital: 2006224, Instancia: Pleno, Décima Época, Materias(s): Constitucional, Tesis: P./J. 20/2014 (10a), Fuente: *Gaceta del Semanario Judicial de la Federación*. Libro 5, abril de 2014, Tomo I, página 202, Tipo: Jurisprudencia. DERECHOS HUMANOS CONTENIDOS EN LA CONSTITUCIÓN Y EN LOS TRATADOS INTERNACIONALES. CONSTITUYEN EL PARÁMETRO DE CONTROL DE REGULARIDAD CONSTITUCIONAL, PERO CUANDO EN LA CONSTITUCIÓN HAYA UNA RESTRICCIÓN EXPRESA AL EJERCICIO DE AQUÉLLOS, SE DEBE ESTAR A LO QUE ESTABLECE EL TEXTO CONSTITUCIONAL.

las disposiciones, propósitos y objetivos del Pacto", por lo que la expresión "injerencias arbitrarias" se hace extensiva a las injerencias que estén previstas en la ley.[48]

109. Con relación al concepto de arbitrariedad, el Comité de Derechos Humanos señaló en el párrafo 4, que: "*se pretende garantizar que incluso cualquier injerencia prevista en la ley esté en consonancia con las disposiciones, los propósitos y los objetivos del Pacto, y sea, en todo caso, razonable en las circunstancias particulares del caso*"; la proporcionalidad aludida por el Comité fue interpretada en el sentido de que "*cualquier injerencia en la vida privada debe ser proporcional al propósito perseguido y necesaria en las circunstancias particulares del caso*"[49].

110. En el mismo tenor, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos señaló que "*las injerencias permitidas* [por] *la legislación nacional, pueden no obstante, ser ilegales si dicha legislación nacional es contraria a las disposiciones del Pacto Internacional de Derechos Civiles y Políticos*"[50].

111. Si bien el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos no establece limitaciones explícitas, la Observación General 31 del Comité de Derechos Humanos señala que los Estados parte deben abstenerse de violar los derechos reconocidos por el Pacto y que "*cualesquiera restricciones a cualquiera de* [esos] *derechos deben estar permitidas según las disposiciones pertinentes del Pacto. Cuando se hacen tales restricciones, los Estados deben demostrar su necesidad y sólo tomar medidas que sean proporcionales a la consecución de objetivos legítimos para garantizar protección continua y efectiva de los derechos del Pacto*".[51]

112. En ese sentido, el margen de discrecionalidad permitido por la Ley de Seguridad Nacional también advierte de las siguientes consideraciones: los artículos 33 y 35 de la referida Ley establecen que, en los casos de amenaza inminente de acuerdo con las

48 Párrafos 3 y 4.
49 Comunicación No. 488/1992, *Toonan C. Australia*, párr. 8.3.
50 Informe: "El Derecho a la privacidad en la era digital"; párrafo 21.
51 *Ibídem*, párr. 22.

hipótesis previstas en el artículo 5, el Poder Judicial de la Federación autorizará al Centro la intervención de comunicaciones privadas.

113. Las fracciones de la I a la XII, del artículo 5 de la Ley de Seguridad Nacional establecen cuales son los actos considerados amenazas a la seguridad nacional, entre los que destaca por su generalidad y ambigüedad la prevista en la fracción XI: "Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia".

114. Aunque el artículo 29 de la Ley de Seguridad Nacional describe qué se entiende por "inteligencia", esta definición únicamente atiende a un contenido teórico, igualmente genérico y amplio, que permite una interpretación y aplicación discrecional a cargo del Centro al momento de fundamentar en dicha hipótesis normativa la solicitud de intervención de comunicaciones ante la autoridad judicial.

115. En efecto, si se considera que "inteligencia" es definida como "*el conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de información para la toma de decisiones en materia de seguridad nacional*", se observa que cualquier acto, inclusive los desarrollados en ejercicio del derecho a la libertad de expresión y el derecho a defender, pudieran ser indebidamente considerados por el Centro como argumento para solicitar la intervención de comunicaciones privadas, con fundamento en la fracción XI, del artículo 5 de la Ley de Seguridad Nacional, lo que evidencia que una solicitud con tales características no satisface los presupuestos de legitimidad, proporcionalidad, necesidad e idoneidad.

116. Ejemplo de un caso que se originó en una situación semejante a la expuesta, es citado en el "Informe Anual 2013 de la Relatoría Especial para la Libertad de Expresión" de la Comisión Interamericana de Derechos Humanos, relativo a la intervención de comunicaciones realizada en 2013 por el Departamento de Justicia de EEUU a la agencia de noticias The Associated Press, con la cual obtuvo registros telefónicos de más de 20 líneas utilizadas por editores y periodistas, entre los que se incluían llamadas realizadas desde las oficinas del medio, así como de las líneas telefónicas personales de varios colaboradores de esa agencia. Estos hechos motivaron que el director de la

agencia de noticias enviara una carta de protesta a la Fiscalía General en la que objetó la intrusión del Departamento de Justicia en las actividades de recolección de noticias en los términos siguientes: "*estos registros potencialmente revelan comunicaciones con fuentes confidenciales a través de todas las actividades de recolección de noticias realizadas por la AP (…) y revelan información acerca de las actividades y operaciones de la AP que el gobierno no tiene derecho concebible a conocer*".[52]

117. En respuesta, el Fiscal General Adjunto manifestó al Director del medio que el Departamento de Justicia "*se esfuerza por alcanzar en cada caso un equilibrio adecuado entre el interés público por la libre circulación de la información y el interés público por la protección de la seguridad nacional y la aplicación efectiva de las leyes penales*". Adicionalmente, en conferencia de prensa, el Fiscal General declaró que tales acciones "*se tomaban en el marco de una investigación sobre una 'filtración muy seria' de información que puso al 'pueblo americano en riesgo', por lo que tratar de determinar quién fue el responsable requería acciones muy firmes*".[53]

118. Otro caso similar es el del periodista James Rosen, corresponsal en Washington de la cadena televisiva Fox News, cuyos correos electrónicos y registros telefónicos fueron intervenidos por el FBI, y sus visitas al Departamento del Estado rastreadas en el marco de una investigación iniciada en 2010 contra el asesor del Departamento de Estado Stephen Jin-Woo Kim, acusado de violar la Ley de Espionaje de 1917, por presuntamente haber filtrado información clasificada vinculada a Corea del Norte, en 2009.

119. El Washington Post publicó el 19 de mayo de 2013 la orden judicial que autorizó la inspección del correo electrónico del periodista, así como la solitud presentada al juez por un agente especial del FBI, en la cual se cataloga al periodista como "*un colaborador, cómplice y/o conspirador*" en el caso de espionaje. Así, el juez federal habría autorizado

52 Párrafo 425.
53 *Ídem*.

la intervención sobre la base de “causa probable” de la participación del periodista en el delito.[54]

120. Con anterioridad a los casos citados, ya se habían documentado e investigado otros casos análogos, como el *Caso Molina Theissen vs. Guatemala* en el que la Corte Interamericana de Derechos Humanos señaló que la llamada “Doctrina de Seguridad Nacional” permitía calificar a una persona como “subversiva” o “enemiga interna” por el sólo hecho de que, real o presuntamente, respaldara la lucha para cambiar el orden establecido.[55]

121. Igualmente, en el *Caso Goiburú y otros Vs. Paraguay*, la Corte Interamericana advirtió que: “[l]*a mayoría de los gobiernos dictatoriales de la región del Cono Sur asumieron el poder o estaban en el poder durante la década de los años setenta* […]*. El soporte ideológico de todos estos regímenes era la ‘doctrina de seguridad nacional’ por medio de la cual visualizaban a los movimientos de izquierda y otros grupos como ‘enemigos comunes’.*[56]

122. Al retomar lo antes expuesto sobre la Ley de Seguridad Nacional, la Comisión Nacional de los Derechos Humanos advierte que el artículo 49 permite que el procedimiento establecido para solicitar la intervención de comunicaciones no sea agotado en todos los casos. Basta que el Centro manifieste la “urgencia” derivada solamente de “indicios” para que el juez federal inmediatamente deba conceder la autorización para la ejecución de tal medida, lo cual implica que dicha norma otorga un poder excesivo a un órgano de inteligencia, estableciendo inclusive una “obligación” hacia el órgano jurisdiccional.

123. Sobre este punto, es importante advertir que la excepción prevista en el artículo 49 de la Ley de Seguridad Nacional puede ser conculcatoria del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, ya que la razón de que el

54 *Ibidem*. párr.426.
55 SCJN. Sentencia de 4 de mayo de 2004. Fondo. párr. 40.2.
56 SCJN. Sentencia de 22 de septiembre de 2006. Fondo, Reparaciones y Costas.153. párr. 61.5.

precepto constitucional haya sujetado la procedencia de la intervención de comunicaciones a la determinación del Poder Judicial de la Federación obedece al carácter lesivo que por sí misma conlleva dicha medida, por lo cual tiene un carácter excepcional que exige al juez realizar un ejercicio de ponderación exhaustivo de los derechos humanos que están en conflicto, así como de las alternativas que pudieran ser empleadas y resultaren menos lesivas para los derechos fundamentales.

124. En atención a ello, es inconcuso que los "indicios" a los que alude el referido artículo 49 no pueden referirse a "sospechas o conjeturas" realizadas por el órgano de inteligencia, sino a información o datos que, apreciados judicialmente, permitan determinar de manera lógica y razonable, conforme a las normas de la experiencia, la probable responsabilidad de una persona con relación a un hecho que puede ser objeto de investigación penal. El juez federal tiene el deber de valorar la procedencia de la solicitud que le sea planteada en términos del artículo 49 de la Ley de Seguridad Nacional en función de criterios de racionalidad y proporcionalidad.

125. Lo anterior se fortalece al considerar que el Poder Judicial de la Federación ha establecido que la prueba indiciaria debe satisfacer cuatro elementos para lograr un ánimo de convicción respecto al hecho al cual se vincula: "*1) que los hechos que se toman como indicios estén acreditados, pues no cabe construir certeza sobre la base de simples probabilidades; 2) que concurra una pluralidad y variedad de hechos demostrados, generadores de esos indicios, 3) que guarden relación con el hecho que se trata de demostrar, y 4) que exista concordancia entre ellos.*"[57]

126. Por lo anterior, los "indicios" a los que se hace referencia en el artículo 49 de la Ley de Seguridad Nacional, de acuerdo con los parámetros citados, implicaría la posibilidad de que éstos pudieran dar origen a una investigación penal, puesto que se originan en la acreditación de hechos vinculados a la probable comisión de una conducta ilícita.

57 Tribunales Colegiados de Circuito. Jurisprudencia penal. "*Prueba indiciaria. Naturaleza y operatividad*". *SEMANARIO JUDICIAL DE LA FEDERACIÓN*, septiembre 2009, registro 166315.

127. Por ello, se subraya que la actual redacción del artículo 49 de la Ley de Seguridad Nacional abre la puerta a posibles injerencias arbitrarias e ilegales por parte del Centro, bajo el argumento de "casos urgentes", así señalados por la legislación en cita, debiéndole corresponder al Poder Judicial de la Federación emitir, en todos los casos y especialmente tratándose de "casos urgentes", una resolución conforme a criterios de racionalidad y proporcionalidad, en la que se realice un ejercicio de interpretación armónica de los estándares internacionales y la legislación interna, antes de que se ejecute la intervención de comunicaciones. Esto servirá como una actividad de "control" ante un posible ejercicio abusivo de la facultad que tiene el Centro conforme a la norma en análisis.

128. Se reitera que el aludido "caso urgente" establecido en la Ley de Seguridad Nacional, no puede ser empleado para justificar de manera alguna la aplicación inmediata de una medida tan lesiva de los derechos humanos como es la intervención de comunicaciones privadas, sin que haya de manera previa a su ejecución, un análisis exhaustivo del juez federal conforme a los criterios descritos.

129. Aunado a lo anterior, esta Comisión Nacional advierte que, aunque el artículo 41, párrafo segundo, de la Ley de Seguridad Nacional establece que el juez podrá requerir informes periódicos al Centro, dicha facultad se circunscribe exclusivamente a la ejecución de la autorización y, en su caso, a la información obtenida, pero no se establece que tal facultad pueda ser ejercida con relación al uso y destino de los datos e información que obtenga el Centro por la intervención de comunicaciones.

130. Lo anterior se constata de la lectura del artículo 47 de la Ley de Seguridad Nacional, el cual prevé que toda la información obtenida con motivo de la intervención de comunicaciones es propiedad del Centro, se encuentra clasificada como reservada y su destino final será determinado por el Consejo de Seguridad Nacional.[58]

58 De acuerdo al artículo 12 de la Ley de Seguridad Nacional, el Consejo de Seguridad coordina las acciones orientadas a preservar la Seguridad Nacional y se integra por el Titular del Ejecutivo Federal; el Secretario de Gobernación; el Secretario de la Defensa Nacional; el Secretario de Marina; el Secretario de Seguridad Pública, actualmente Comisionado Nacional de Seguridad; el Secretario de Hacienda y Crédito Público; el Secretario de la Función Pública; el Secretario de Relaciones Exteriores; el Secretario de

131. En tal virtud, es notorio que la Ley de Seguridad Nacional permite un margen de discrecionalidad no solamente respecto a las solicitudes, control y ejecución de las intervenciones de comunicaciones a cargo del Centro, sino también al uso y destino final de la información que sea obtenida con motivo de tales injerencias a la vida privada. Actualmente, no existen mecanismos de control, supervisión y evaluación que garanticen que el órgano de inteligencia ejerza su facultad en estricto acatamiento al derecho internacional de los derechos humanos.

132. Al respecto, el Relator Especial de las Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión de las Naciones Unidas y la entonces Relatora Especial para la Libertad de Expresión de la CIDH de la OEA, en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión, señalaron que cuando se cite la seguridad nacional como razón para efectuar actos de vigilancia que limiten el derecho a la privacidad, la ley debe especificar claramente los criterios que se aplicarán para determinar los casos en los cuales este tipo de limitaciones resulta legítimo, por el riesgo cierto respecto a los intereses protegidos y cuando ese daño sea superior al interés general de la sociedad, en función de mantener el derecho a la privacidad y a la libre expresión de pensamiento y circulación de información.[59]

133. Este Organismo Nacional también advierte que el Ministerio Público, sea federal o local, tiene la facultad discrecional para utilizar esta medida en la investigación de delitos, sean o no graves, sin que la ley establezca criterios expresos para la elección de "objetivos", ni se prevea la obligación de notificar, en su oportunidad y de ser posible, a la persona que ha sido objeto de tal injerencia a su vida privada. Tampoco se regulan los mecanismos para el debido resguardo de los registros que corresponden a las intervenciones de comunicaciones, particularmente, de aquellos que pudieran acreditar responsabilidades administrativas y/o penales a cargo del Ministerio Público.

Comunicaciones y Transportes; el Fiscal General de la República, y el Director General del Centro.
59 21 de junio de 2013, punto 9.

134. Del contenido del artículo 291 del Código Nacional de Procedimientos Penales se concluye que, a diferencia del numeral 278 Ter del Código Federal de Procedimientos Penales[60], la calidad de "grave" en el delito, ya no es requerida para que el Ministerio Público ejecute la intervención de comunicaciones privadas. Aunque para ello es necesario que se solicite autorización al Poder Judicial de la Federación; el plazo máximo de seis horas que prevé el tercer párrafo del artículo 291 en cita para que el juez federal resuelva la solicitud correspondiente es insuficiente para que se realice un análisis exhaustivo respecto a los principios de legalidad, necesidad, proporcionalidad e idoneidad de cada caso en que la autorización de tal medida le sea solicitada. Con ello, se desarticula la posibilidad de que el Poder Judicial de la Federación pueda constituirse en un medio o mecanismo de control respecto al ejercicio de tales atribuciones del Ministerio Público. No obstante, ante una situación urgente, tendría que mediar un análisis que evidenciara que la medida autorizada no fue desproporcionada, ni violentó los principios señalados.[61]

60 Abrogado en los términos establecidos en el artículo tercero transitorio del Código Nacional de Procedimientos Penales, el 5 de marzo de 2014.

61 El artículo 291 del Código Nacional de Procedimientos Penales regula el presupuesto general de la facultad del Ministerio Público para la intervención de comunicaciones. Este numeral señala que corresponderá al Procurador General de la República o a quienes delegue esta facultad, así como a los procuradores de las entidades federativas, solicitar al juez federal de control competente, la autorización para la ejecución de tal medida. Al respecto, se precisa que conforme a los artículos Segundo, fracción V; Tercero, Quinto y Sexto del Acuerdo del Procurador General de la República A/018/15, publicado en el Diario Oficial de la Federación, el 23 de febrero de 2015, las siguientes autoridades tienen facultad expresa para solicitar la intervención de comunicaciones privadas por delegación de facultades del titular de la Procuraduría General de la República: TERCERO: **I.** Subprocuraduría Jurídica y de Asuntos Internacionales; **II.** Subprocuraduría de Control Regional, Procedimientos Penales y Amparo; **III.** Subprocuraduría Especializada en Investigación de Delincuencia Organizada; **IV.** Subprocuraduría Especializada en Investigación de Delitos Federales; **V.** Subprocuraduría de Derechos Humanos, Prevención del Delito y Servicios a la Comunidad; **VI.** Visitaduría General; **VII.** Fiscalía Especializada para la Atención de Delitos cometidos contra la Libertad de Expresión; **VIII.** Fiscalía Especializada en materia de Delitos relacionados con Hechos de Corrupción; **IX.** Fiscalía Especializada para los Delitos de Violencia contra las Mujeres y Trata de Personas; **X.** Unidad Especializada en Investigación de Delitos contra la Salud; **XI.** Unidad Especializada en Investigación de Terrorismo, Acopio y Tráfico de Armas; **XII.** Unidad Especializada en Investigación de Operaciones con Recursos de Procedencia Ilícita y de Falsificación o Alteración de Moneda; **XIII.** Unidad Especializada en Investigación de Delitos en materia de Secuestro; **XIV.** Unidad Especializada en Investigación de Tráfico de Menores, Personas y Órganos; **XV.** Unidad Especializada en Investigación de Asalto y Robo de Vehículos; **XVI.** Unidad Especializada en Investigación de Delitos contra los Derechos de Autor y la Propiedad Industrial; **XVII.** Unidad Especializada en Investigación de Delitos Fiscales y Financieros; **XVIII.** Unidad Especializada en Investigación de Delitos Cometidos por Servidores Públicos y contra la Administración de Justicia; **XIX.** Unidad Especializada en Investigación de Delitos de Comercio de Narcóticos destinados al Consumo Final; **XX.** Unidad Especializada en Investigación de Delitos contra el Ambiente y Previstos en Leyes Especiales; Coordinación de Control y Supervisión Regional. QUINTO. Director en Jefe de la Agencia de Investigación Criminal. SEXTO. Agentes del Ministerio Público de la Federación, previa autorización del titular de la Unidad Administrativa a la que se encuentre adscrito.

135. Sobre lo anterior, un sector doctrinario advierte que la obligación de que la resolución judicial que autoriza la intervención de comunicaciones se encuentre debidamente motivada es una exigencia constitucional y no solamente legal. En ese sentido considera que el juez debe expresar en la resolución correspondiente:

> […] *el juicio de ponderación sobre la necesidad de la injerencia, atendiendo diversos aspectos directamente vinculados con el principio de proporcionalidad, ya que la intervención de comunicaciones privadas solo se debe utilizar como un medio supletorio y excepcional de investigación, que exige considerar, ante todo, la previa existencia de indicios de criminalidad, es decir, la existencia de una sospecha razonable de la comisión de una infracción grave por una persona determinada.[…] esta exigencia sólo puede considerarse plenamente satisfecha cuando […] permite conocer, de manera suficientemente precisa, los criterios esenciales de la decisión, lo cual obliga a realizar no solo una detallada exposición de los hechos objeto de la investigación y de las circunstancias del delito investigado, sino también a indicar cuáles son los indicios que sirven de fundamento a la sospecha existente contra el imputado, si puede suponerse, razonablemente, que con la escucha se obtendrá la prueba de la realización del delito, y si se han ensayado otros medios de investigación menos lesivos para la intimidad del investigado, si éstos han fracasado, o es probable que fracasen, o serían demasiados peligrosos para la seguridad de los agentes, pues sólo a través del enjuiciamiento de todas estas circunstancias es posible verificar, en cada caso, si se han respetado las exigencias derivadas del principio de proporcionalidad y necesidad de la injerencia*. [62]

136. La exigibilidad de una resolución judicial que agote en su análisis la plena satisfacción de los principios invocados adquiere una trascendencia particular, ya que de acuerdo con las disposiciones del Código Nacional de Procedimientos Penales, las injerencias a la vida privada no se circunscriben a las comunicaciones de las personas indiciadas o probables responsables de la comisión de un delito. Por el contrario, la facultad establecida en la norma a favor del Ministerio Público es amplia, irrestricta y no

62Vicenta Ángeles Zaragoza Teuler, “Intervención de las comunicaciones: puntuales aspectos sustantivos y procesales.” Alicante, España, 6 de agosto de 2003.

establece una calidad específica de la persona que será objeto de tal intervención, tampoco del delito asociado a la investigación.

137. Aunado a ello, no hay disposiciones que establezcan la obligación del Ministerio Público de notificar, en algún momento del procedimiento judicial, la ejecución de tal medida a la persona que ha sido objeto de actos de vigilancia. Esto implica una violación a los derechos humanos de legalidad, seguridad jurídica y debido proceso; en atención a que de acuerdo con los Principios Internacionales sobre la aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, toda persona afectada en su derecho humano a la privacidad por actos de vigilancia ejecutados por el Estado debe ser notificada de la determinación judicial que autorizó tal medida, una vez que su finalidad haya sido satisfecha. Dicha notificación debe precisar cuáles fueron los elementos presentados para sustentar la solicitud de autorización, así como la información personal que fue obtenida.

138. Esta notificación tiene por finalidad asegurar que la persona afectada pueda promover las acciones de defensa que considere necesarias en contra de tal autorización. Aunque los principios referidos no prevén un plazo específico para realizar dicha notificación, establecen que debe hacerse con “tiempo suficiente” para el ejercicio de acciones de defensa y que sólo se admite su “retraso”, en las siguientes circunstancias: a) cuando la notificación ponga seriamente en peligro el propósito por el cual se autoriza la vigilancia de las comunicaciones o haya un riesgo inminente de peligro para la vida humana; b) cuando la autorización para retrasar la notificación sea concedida por la autoridad judicial competente, y c) cuando 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.[63]

63 Principios Internacionales sobre la aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponible en https://web.karisma.org.co/wp-content/uploads/2014/03/13Principios_es.pdf.

139. No pasa inadvertido para este Organismo Nacional, que el artículo 300 del Código Nacional de Procedimientos Penales establece la destrucción de los registros de intervenciones de comunicaciones privadas por orden del órgano jurisdiccional en los siguientes casos: a) cuando no se relacionen con los delitos investigados o con otros delitos que hayan ameritado la apertura de una investigación diversa; b) cuando la intervención "rebase" los términos de la autorización judicial respectiva, y c) cuando se decrete el archivo definitivo, sobreseimiento o la absolución del imputado.

140. El contenido del artículo en cita corrobora que, la autorización otorgada por el Poder Judicial de la Federación para la intervención de comunicaciones privadas en la forma en que actualmente se encuentra regulada, es insuficiente para garantizar la legalidad y proporcionalidad de tal injerencia. Es preocupante, además, que la ley prevea la destrucción de registros de intervenciones de comunicaciones que "no se relacionen con la investigación" que motivó su autorización o que "rebase los términos de la autorización judicial", hipótesis que implica un uso ilegal y arbitrario de tal medida, ya que presuponen que su ejecución por el Ministerio Publico no se constriñó o ajustó a los extremos ni de la solicitud de la autorización, ni de la resolución judicial dictada para tal efecto. Por ello es importante su conservación, al menos durante el plazo necesario para que la persona afectada por tal acto de autoridad pueda ejercer las acciones legales correspondientes.

141. En efecto, contrario a lo establecido en el numeral de referencia, la ley tendría que determinar que tales registros debieran ser resguardados por el órgano judicial con la finalidad de notificar a la persona afectada. Lo anterior con la finalidad de que ésta se encuentre en posibilidad de ejercer las acciones legales correspondientes. Esto en virtud de que dichos registros constituyen pruebas relativas a la posible responsabilidad administrativa e inclusive penal del Ministerio Público por injerencias ilegales y arbitrarias.

142. En este sentido, el Relator Especial para la Libertad de Expresión en el Informe Anual de 2016 refirió que el uso de tecnologías para la vigilancia, intervención y recolección de datos, al ser altamente intrusivas, debían ser empleadas únicamente en

el contexto de la investigación de delitos graves, ya que el requisito legal de la autorización judicial para su ejecución “no es suficiente garantía, sin un marco legal adecuado, mecanismos mínimos de transparencia y conocimiento técnico especializado por parte de los jueces competentes”.[64]

143. Respecto a la regulación de la intervención de comunicaciones privadas en el ámbito de competencia de la justicia castrense, prevista en los artículos: 287 a 298 del Código Militar de Procedimientos Penales vigente, son aplicables las mismas observaciones que se han realizado a la regulación que contempla el Código Nacional de Procedimientos Penales, en tanto que estas disposiciones constituyen una fiel reproducción de aquéllas, diferenciándose exclusivamente en su ámbito militar de aplicación.

144. Como se advierte en los casos citados, la gran variedad de hechos y situaciones que pudieran ser interpretadas discrecionalmente y, por ende, de manera inadecuada por los órganos de inteligencia y de procuración de justicia como “amenazas a la seguridad nacional”, aunada a las de normas generales, ambiguas y/o deficientes, así como a la ausencia de mecanismos de evaluación, control y seguimiento tanto en las solicitudes como en la ejecución de intervenciones de comunicaciones, propician la posibilidad de injerencias ilegales y arbitrarias en la vida privada.

145. Con ello se acredita que hay un riesgo para la sociedad misma, particularmente para los periodistas, comunicadores y personas defensoras, derivado de la posibilidad de que se apliquen actos de vigilancia que intervengan con el derecho a la privacidad más allá de lo estrictamente necesario para lograr fines legítimos de seguridad nacional, generando así un efecto amedrentador en el derecho de buscar, recibir y difundir información e ideas de toda índole, así como en las acciones necesarias para ejercer libremente el derecho a defender derechos humanos, tal y como lo advirtieron diversas organizaciones de la sociedad civil.[65]

64 Párrafos 1289 y 1290.
65 CIDH; 149 Periodo de Sesiones. Audiencia: Libertad de expresión y vigilancia de comunicaciones por parte de Estados Unidos;

B.2. Deficiencia por normas vagas o ambiguas o inexistentes

146. La Ley de Seguridad Nacional abre la posibilidad a la ejecución de injerencias arbitrarias e ilegales, por el hecho de que la redacción de los actos previstos en las fracciones II, IV, VII y XI del artículo 5 de la Ley en cita, reflejan ambigüedad, ya que algunas de estas hipótesis pueden abarcarse por la legislación penal y otras no.[66]

147. Esta ambigüedad posibilita que el órgano de inteligencia realice investigaciones empleando tecnologías para la vigilancia de comunicaciones privadas, bajo el argumento de probables actos que constituyen amenazas a la seguridad nacional, con fundamento en las citadas fracciones II, IV, VII y XI, del artículo 5 de la Ley de Seguridad Nacional, sin que necesariamente esos "actos" sean considerados por las autoridades judiciales como delitos, dada la referida ambigüedad de tales hipótesis normativas.

148. Al respecto, cabe destacar que el Principio 20, denominado "Protecciones generales del imperio de la ley", de los "Principios de Johannesburgo sobre la Seguridad Nacional, la libertad de expresión y el acceso a la información", establece que: "*toda persona acusada de un delito relativo a la seguridad y que involucre la expresión o la información tiene derecho a todas las protecciones del imperio de la ley que forman parte del derecho internacional. Éstas incluyen, pero no se limitan, a los siguientes derechos: (a) el derecho*

28 de octubre de 2013.

66 La fracción II del artículo 5 de la Ley citada, considera amenaza a la seguridad nacional los actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado mexicano; lo que, dependiendo del caso, puede ser constitutivo del delito de espionaje previsto en el artículo 127 del Código Penal Federal, el cual sanciona al extranjero que en tiempo de paz, con objeto de guiar a una posible invasión del territorio nacional o de alterar la paz interior, tenga relación o inteligencia con persona, grupo o gobierno extranjeros o le dé instrucciones, información o consejos. Asimismo, al extranjero que en tiempo de paz proporcione sin autorización, a persona, grupo o gobierno extranjero, documentos, instrucciones, o cualquier dato de establecimientos o de posibles actividades militares.

La fracción IV contempla los actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos; lo que puede constituir una modalidad del delito de traición a la Patria previsto en el artículo 123 del Código Penal Federal, que sanciona a quien realice actos contra la independencia, soberanía o integridad de la Nación mexicana con la finalidad de someterla a persona, grupo o gobierno extranjero.

La fracción VII refiere actos que atenten en contra del personal diplomático; en este caso y con independencia de poder configurar algún otro tipo de ilícito, según la naturaleza del acto concreto que se realice, podría configurarse el delito de violación de inmunidad diplomática previsto en el artículo 148 del Código Penal Federal.

Finalmente, la fracción XI hace alusión a los actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, que son los únicos que no tienen un encuadramiento exacto en la ley penal, pero que eventualmente pudieran relacionarse con el delito de espionaje.

de ser presumido/a inocente; (b) el derecho a no ser arbitrariamente detenido/a; (c) el derecho a ser informado/a, en el más breve plazo y en una lengua que pueda comprender, de las acusaciones y de la prueba justificativa contra él o ella; (d) el derecho a acceso en el más breve plazo a un/a defensor/a de su elección; (e) el derecho a un juicio dentro de un plazo razonable; (f) el derecho a disponer del tiempo adecuado para la preparación de su defensa; (g) el derecho a que su causa sea oída justa y públicamente por un tribunal o juzgado independiente imparcial; (h) el derecho a interrogar a los testigos de cargo; (i) el derecho a que el testimonio no sea introducido en el juicio a no ser que haya sido divulgado al/a la acusado/a y que él o ella haya tenido la oportunidad de refutarlo; y (j) el derecho a apelar a un juzgado o tribunal independiente que tenga el poder de revisar el fallo de acuerdo con la ley y los hechos y de anularlo."[67]

149. En este pretendido esquema de "inteligencia estratégica", los gobiernos emplean tecnologías que les permiten realizar actos de vigilancia masiva, lo que es incompatible con los sistemas democráticos. Como se ha expuesto en párrafos precedentes, la facultad de los gobiernos para intervenir comunicaciones privadas en la investigación de amenazas a la seguridad nacional o de delitos graves, es permisible si y sólo si la autoridad satisface tanto en la solicitud como en la ejecución y control de tal medida los principios del derecho internacional de los derechos humanos.

150. Esto quiere decir que los gobiernos podrán emplear tecnologías de vigilancia únicamente bajo los principios de legalidad, necesidad, proporcionalidad e idoneidad, respecto a un objetivo individualizado y sólo por un tiempo determinado, cuando haya indicios razonables que deriven de hechos ciertos, debidamente valorados por una autoridad judicial independiente.

151. Hay una problemática que deriva de la descripción de la información que se clasifica como reservada por motivos de seguridad nacional. El artículo 51 de la Ley de Seguridad Nacional prevé que además de la información que satisfaga los criterios establecidos en la legislación general aplicable, es información reservada: "*I. Aquella cuya aplicación*

67 Artículo 19. Londres, Reino Unido, 1996, ed. Español 2005.

implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen o; II. Aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza".

152. Adicionalmente, el artículo 37 de la Ley de Seguridad Nacional establece que el procedimiento relativo a la intervención de comunicaciones privadas en materia de seguridad nacional es reservado y prohíbe de manera expresa, el acceso a los expedientes correspondientes, a excepción del secretario del Juzgado y de "quien se autorice por escrito por parte del Director General del Centro".

153. Esta "secrecía", no sólo del procedimiento de intervención de comunicaciones privadas y de la información relativa a la "causa del pedimento", selección del objetivo, datos obtenidos, su uso y destino, sino también de los "métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia", evidencia que se dan condiciones, amparadas por el marco normativo, que posibilitan la práctica de injerencias ilegales y arbitrarias.

154. Sobre este punto, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos apunta que el Estado debe asegurar que toda injerencia al derecho a la vida privada de las personas se funde y motive en leyes que satisfagan los siguientes principios: a) sean de acceso público; b) contengan disposiciones que garanticen que la obtención, el acceso y la utilización de los datos de las comunicaciones obedezcan a objetivos específicos legítimos; c) sean suficientemente precisas y especifiquen en detalle las circunstancias concretas en que dichas injerencias pueden ser autorizadas, los procedimientos de autorización, las categorías de personas que pueden ser sometidas a vigilancia, el límite de la duración de la vigilancia y los procedimientos para el uso y el almacenamiento de los datos recopilados, y d) proporcionen salvaguardas efectivas contra el uso indebido.[68]

68 Informe: El Derecho a la privacidad en la era digital, párr.28.

155. Por ello, de manera enfática el Alto Comisionado de las Naciones Unidas para los Derechos Humanos observa que las normas e interpretaciones "secretas" del derecho no cumplen con los requisitos necesarios para considerarse "ley", ya que el carácter "secreto" de determinadas facultades de vigilancia involucra un mayor riesgo de ejercicio arbitrario de la discrecionalidad, lo cual exige una mayor precisión en la norma, así como mayor supervisión.[69]

156. Al respecto, este Organismo Nacional reitera que, debido a la interpretación discrecional que puede realizar el órgano de inteligencia de hechos o circunstancias que asocie con amenazas a la seguridad nacional, así como a la falta de criterios que de manera taxativa establezcan qué conductas constituyen delitos por motivos de seguridad nacional, es apremiante realizar una reforma legislativa en materia de seguridad nacional, particularmente, con relación a las facultades de vigilancia, intervención y recolección de datos de los órganos de inteligencia, a fin de que se incorporen estándares internacionales de derechos humanos.

B.3. Deficiencia por la falta de regulación sobre los tipos y alcances de tecnologías para la intervención de comunicaciones, y de los controles para su uso

157. El uso de tecnologías para la vigilancia, intervención y recolección de datos que emplean las autoridades responsables de procuración de justicia, tampoco se encuentra regulado de manera adecuada y concordante con el derecho internacional de los derechos humanos. En efecto, no hay disposiciones que establezcan de manera específica el tipo y alcances de las tecnologías utilizadas para la intervención de comunicaciones, los procedimientos para su adquisición, y los controles aplicables al uso de esas tecnologías.

158. Recordemos que la doctrina de la seguridad nacional resurge en la actualidad con el argumento de la "lucha contra el terror" o "guerra contra el terrorismo", y es en este

69 *Ibidem*, párr. 29.

contexto en el que los gobiernos van normalizando el uso de medidas que antes eran consideradas como una "excepción"; tal es el caso de la vigilancia masiva. Así, el estado de "excepción" lentamente se va convirtiendo en la "regla", como lo señalan diversos autores, como el jurista alemán Günter Frankenberg.[70]

159. En tanto que el jurista italiano Luigi Ferrajoli, advierte que la vigilancia masiva erosiona el principio de legalidad y con él, el Estado de derecho: "*las democracias corren el riesgo –sin garantías civiles sustanciales– de convertirse en una 'cáscara vacía, formal' detrás de la cual no hay una sociedad civil que ejerza plenamente sus derechos políticos. El espionaje erosiona y socava la autonomía personal. Violenta nociones elementales de lo que entendemos por Estado de derecho y democracia constitucional*".[71]

160. Mientras que los autores Zaffaroni y Croxatto, señalan que las diversas posibilidades de "agresión" que abren las nuevas tecnologías de que disponen los estados "[…] parece ser la única forma de preservar la democracia de amenazas no tanto externas ('la amenaza del terrorismo') sino internas, como el espionaje masivo tecnológico, que en nombre del combate del terror y la defensa de las libertades civiles termina socavando esas mismas garantías básicas y esas mismas libertades, en cuyo nombre, paradójicamente, se ejerce y comete. El espionaje masivo termina socavando la libertad y el Estado de Derecho, erosiona la legalidad".[72]

161. De acuerdo a lo anterior, resulta evidente que las nuevas tecnologías facilitan la ejecución de la vigilancia masiva, con los graves efectos y consecuencias que esta medida conlleva para los sistemas democráticos. A pesar de ello, se reitera que del análisis de las normas de derecho interno que autorizan la intervención de comunicaciones privadas, ya sea por motivos de seguridad nacional o bien para la investigación de delitos, se advierte que no hay disposiciones que regulen de manera específica el tipo y alcances de las tecnologías que pueden ser utilizadas para la ejecución de actividades de vigilancia, intervención y recolección de datos. Tampoco hay

70 G. Frankenberg, *Técnica estatal. Perspectivas del estado de derecho y el estado de excepción*; Rubinzal-Culzoni; 2014; en: Zaffaroni, y Croxatto, Óp. cit., pág. 357.
71 L. Ferrajoli, *Democracia y garantismo;* Madrid; Trotta, 2012, en Zaffaroni y Croxatto, Óp. cit., pág. 357.
72 *Óp. cit*., pp. 356 y 357.

una regulación respecto a los procedimientos para su adquisición, ni con relación a la selección de objetivos, el manejo de los datos obtenidos y controles aplicables al uso de dichas tecnologías.

162. Lo anterior es así, ya que actualmente los estados cuentan con la posibilidad de realizar actividades de vigilancia simultánea, invasiva, con objetivos precisos y a gran escala, debido al desarrollo y venta de estas nuevas tecnologías en el mercado mundial, circunstancia que aumenta el riesgo de que la vigilancia digital escape de controles gubernamentales, tal y como lo ha manifestado la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.[73]

163. Esta omisión es preocupante, ya que como se ha expuesto en el cuerpo de la presente Recomendación General, la intervención de comunicaciones privadas constituye un acto lesivo a derechos humanos. Por tanto, dicha intervención debe ejecutarse de manera excepcional y controlada, mediante salvaguardas establecidas conforme a los estándares internacionales, para evitar así el uso indiscriminado y abusivo de tecnologías de vigilancia masiva.

164. Al respecto, la Corte Interamericana de Derechos Humanos al pronunciarse en los casos *Ivcher Bronstein vs. Perú, y Baena Ricardo y otros vs. Panamá* consideró que el artículo 8 de la Convención Americana, "no limita su aplicación a recursos judiciales sino que debe entenderse como el conjunto de requisitos que se deben observar 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".[74]

165. Bajo el contexto expuesto, se subraya que la generalidad, vaguedad y/o ambigüedad, particularmente de las normas que establecen los actos que constituyen amenazas a la seguridad nacional, posibilita que los gobiernos consideren ciertas actividades de defensa, denuncia pública, búsqueda y publicación de información que

73 Informe: El Derecho a la privacidad en la era digital, párr. 2 y 3.
74 *Caso Ivcher Bronstein vs. Perú*. Fondo, Reparaciones y Costas. Sentencia de 6 de febrero de 2001, párr. 102. *Caso Baena Ricardo y otros vs. Panamá.* Fondo, Reparaciones y Costas. Sentencia de 2 de febrero de 2001, párr. 124.

realice cualquier ciudadano, en especial, periodistas, comunicadores y personas defensoras de derechos humanos como actividades “sospechosas”, “subversivas”, “problemáticas” o “riesgosas” para la seguridad nacional, en virtud de lo cual pudieran realizar actos de vigilancia que excedan los límites legales, con el argumento de que estas medidas son necesarias para obtener información que sea útil para “prevenir” cualquier situación que altere el orden público y la paz social; argumento que no es aceptable bajo ninguna condición en un estado democrático.

166. El Relator Especial de las Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, en el informe publicado el 17 de abril de 2013, puso énfasis en la problemática, en los términos siguientes: “*Aún en la actualidad las razones de seguridad nacional suelen ser invocadas para poner bajo vigilancia a defensores de derechos humanos, periodistas, comunicadores o activistas para justificar un excesivo secretismo en los procedimientos de toma de decisiones y en las investigaciones vinculadas a cuestiones de vigilancia*”.

167. El falaz argumento empleado por los gobiernos para limitar el derecho a la privacidad y libertad de expresión de las personas tiene su origen en el cambio de paradigma que significó el fenómeno globalizador, vinculado al avance y crecimiento de las tecnologías de información y comunicación. Esto modificó sustancialmente las condiciones sociales, políticas, económicas y culturales de las naciones, creándose relaciones de interdependencia, en donde los modelos de inteligencia “tácticos” que habían sido desarrollados bajo un esquema militar para el resguardo de la seguridad nacional vinculada al concepto de defensa del Estado soberano, es sustituido por un modelo de Inteligencia “estratégica”, de naturaleza “preventiva” de conflictos sociales, en el cual el Estado debe obtener información que le permita “anticiparse” a posibles conflictos y lograr así una óptima toma de decisiones.[75]

168. Por lo expuesto, bajo ninguna circunstancia es aceptable que se realicen actos de vigilancia masiva a organizaciones de la sociedad civil, colectivos, activistas, directivos y

75 José Raúl Cáceres, *Inteligencia Estratégica. Visión preventiva y visión proactiva para la decisión*

colaboradores de medios de información, políticos, jueces, comunicadores, estudiantes, entre otros, porque la propia naturaleza de esta clase de vigilancia la sitúa fuera de la ley, al no guardar correspondencia con las hipótesis legales que a nivel constitucional y convencional prevén la intervención de comunicaciones privadas.

B.4. Deficiencia por falta de regulación sobre la contratación, adquisición y responsabilidades de las empresas desarrolladoras de tales tecnologías

169. Es necesario abordar la problemática vinculada a la corresponsabilidad de las empresas que desarrollan y comercializan tecnologías para la vigilancia, intervención y recolección de datos en materia de respeto y tutela de derechos humanos. Durante los años en los que comenzó el desarrollo de las nuevas tecnologías de la información y comunicaciones, México, como la mayoría de los países latinoamericanos carecieron de políticas públicas y normas que permitieran regular de manera eficiente y adecuada las situaciones derivadas de la adquisición y uso de estas tecnologías. En consecuencia, las empresas responsables de su desarrollo y comercialización contaron con un amplio margen de discrecionalidad para determinar las condiciones operativas de las tecnologías en cuestión. Por citar un ejemplo: el hecho de que la ubicación de las personas servidoras públicas donde se almacena información pueda localizarse fuera de territorio nacional, dificulta la investigación de acciones de vigilancia, intervención y/o recopilación de datos.

170. De igual forma, las empresas aprovecharon la omisión de los Estados, derivada de la ausencia de normas legales sobre el establecimiento de cláusulas en los contratos de compra-venta y/o prestación de servicios, mediante las cuales se les vinculara por las posibles violaciones a derechos humanos derivadas del uso, impacto y alcances de las tecnologías desarrolladas y comercializadas por estas empresas; máxime al considerar a aquellas tecnologías elaboradas para objetivos específicos como son la vigilancia, intervención y recopilación de datos, que por sus propias características involucra un grave peligro para el respeto a los derechos humanos.

171. En los *Principios Rectores sobre las Empresas y los Derechos Humanos*, publicados en 2011 por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos[76] y adoptados por el Consejo de Derechos Humanos en la resolución A/HRC/RES/17/4, de 16 de junio de 2011, se establece que las empresas tienen la responsabilidad de respetar los derechos humanos. Por tanto, deben evitar que sus actividades "*provoquen o contribuyan a generar consecuencias negativas en la observancia de los derechos humanos*", así como tratar de prevenir o mitigar las que se ocasionen de manera directa sobre éstos derivadas de las operaciones, productos o servicios prestados como consecuencia de sus relaciones comerciales, incluso cuando no hayan contribuido a generarlas.[77]

172. Adicionalmente, se prevé que para que las empresas asuman su responsabilidad de respetar derechos humanos deben expresar su compromiso mediante una declaración política, que cumpla con los siguientes puntos:[78]

> "*a) Sea aprobada al más alto nivel directivo de la empresa;*
>
> *b) Se base en un asesoramiento especializado interno y/o externo;*
>
> *c) Establezca lo que la empresa espera, con relación a los derechos humanos, de su personal, sus socios, y otras partes directamente vinculadas con sus operaciones, productos o servicios;*
>
> *d) Se haga pública y se difunda interna y externamente a todo el personal, los socios y las otras partes interesadas;*
>
> *e) Quede reflejada en las políticas y procedimientos operacionales necesarios para inculcar el compromiso asumido a nivel de toda la empresa."*

173. Este Organismo Autónomo, a partir de 2018 creó el Programa de Empresas y Derechos Humanos, con la finalidad de incorporar en su agenda de trabajo a las

76 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *Principios Rectores sobre las Empresas y los Derechos Humanos: puesta en práctica del marco de las Naciones Unidas para proteger, respetar y remediar*, 2011.
77 *Ibidem*, Principio número 13. p.17.
78 *Ibidem,* Principio número 16. p.19.

empresas en el respeto a los derechos humanos. El objetivo de dicho Programa es consolidar una cultura preventiva y de respeto a los derechos humanos en las actividades de las empresas, a través de la promoción, el estudio, la formación y la capacitación a las personas servidoras públicas, las personas empresarias y a la población en general. A través de este Programa, la Comisión Nacional de los Derechos Humanos busca crear herramientas y estrategias institucionales para fungir como mecanismo de reparación no jurisdiccional efectivo y accesible para las víctimas y aportar al cumplimiento de los Objetivos de Desarrollo Sostenible de la Agenda 2030.

174. En atención a lo expuesto, la adquisición de cualquier instrumento, herramienta, equipo, *software*, *hardware* o similar por el Estado y su empleo en actividades que, por su naturaleza, pudieran ocasionar la violación a derechos humanos, como es el caso de los utilizados en la vigilancia, intervención y recopilación de datos, deben realizarse conforme a un marco normativo apropiado para prevenir, investigar, castigar y reparar posibles abusos en el uso de estas tecnologías. Dicha reglamentación debe establecer con plena claridad la responsabilidad y las obligaciones de las empresas que desarrollan, producen y comercializan tales tecnologías, en atención a su potencial para atentar contra derechos humanos de manera incluso masiva. México no cuenta, a la fecha, con un marco regulatorio adecuado que prevea los límites y obligaciones de las empresas y sus directivos en materia de derechos humanos y uso de nuevas tecnologías.

175. Sobre este punto, cabe señalar que el “Convenio sobre la Ciberdelincuencia”, popularmente conocido como “Convenio de Budapest”, elaborado en el año 2001 por el Consejo de Europa, se ha consolidado como el principal texto legal sobre cooperación internacional con fines de persecución penal y lucha contra los ciberdelitos. La lista de firmantes incluye 44 Estados miembros del Consejo de Europa y algunos Estados no miembros, como Argentina, Canadá, Chile, Colombia, Estados Unidos de América, República Dominicana y Perú. México a la fecha no ha concretado su adhesión, sin embargo, es importante considerar su incorporación de manera armónica con la

legislación nacional para la investigación de los delitos que pudieran derivar del uso de tecnologías como Pegasus.[79]

176. Igualmente, al respecto destacan los comentarios realizados por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos a los Principios 4 y 17, respecto al nexo entre el Estado y las empresas, así como la debida diligencia en materia de derechos humanos. En efecto, los Estados son los principales sujetos obligados en términos de los estándares internacionales de derechos humanos, y colectivamente los garantes del régimen internacional de derechos humanos, por lo que la satisfacción del principio de debida diligencia a su cargo, implica que alienten y exijan en todas las operaciones comerciales que desarrollen con empresas, que éstas asuman su responsabilidad de respeto a los derechos humanos, identificando, previniendo, mitigando y respondiendo a las consecuencias negativas que hayan provocado o contribuido a provocar, a través de sus actividades, operaciones, productos o servicios prestados por sus relaciones comerciales.[80]

177. La adquisición, sin embargo, de estas nuevas tecnologías por los Estados no satisfacen los estándares mínimos mencionados con antelación, ya que preponderantemente son las condiciones de mercado las que determinan la elección de empresas para contratar servicios o productos que pudieran ser altamente riesgosos para el respeto de los derechos humanos.

178. En el informe: "La vigilancia y los derechos humanos", publicado en 2019, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas señaló que: "*Debido a que las empresas del sector de vigilancia privada operan bajo un manto de secretismo, el público carece de información sobre la forma en que esas empresas determinan –suponiendo que lo hagan– el impacto de sus productos en los derechos humanos. Dada la naturaleza del sector y el uso generalizado de sus productos para fines incompatibles con el derecho internacional de*

[79] Bruna Martins dos Santos, "Convenio de Budapest sobre la Ciberdelincuencia en América Latina", Derechos digitales América Latina, mayo de 2022. pág. 6.
80 *Ibidem*. Principios 4 y 17. Comentarios.

los derechos humanos, es difícil imaginar que en realidad tengan en cuenta ese impacto. Dicho de otro modo: dado el amplio conocimiento público de la represión que practican muchos de sus clientes, las empresas no pueden pretender que les tomen en serio cuando afirman que no tienen conocimiento del uso represivo de sus productos."[81]

179. De la información obtenida para la documentación del presente caso, se advirtió que entre 2011 a 2017, diversas entidades de la Administración Pública adquirieron programas para la intervención de comunicaciones, sin que hayan informado a este Organismo Autónomo, o conste en otras fuentes de información, si la elección de tales programas atendió a criterios específicos sobre su capacidad para captar información, ni le hayan proporcionado estudios o análisis adecuados para su adquisición. Tampoco informaron si hay restricciones de uso solicitadas o previstas en los contratos respectivos, ni salvaguardas a derechos humanos, entre otros aspectos. Lo anterior, aunado al vacío normativo detallado en la presente Recomendación General, evidencia una grave situación de hecho que debe ser urgentemente atendida por el Estado mexicano.

180. De acuerdo con el Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, tanto empresas como particulares y gobiernos llevan a cabo actividades de vigilancia, intervención y recopilación de datos aprovechando no sólo las posibilidades que les proveen las nuevas tecnologías de la información y comunicación, sino también la falta de reglamentación adecuada respecto a su uso y límites, lo que ha facilitado e inclusive propiciado el ejercicio de tales actividades.[82] El Relator Especial sobre la promoción y protección del derecho a la Libertad de Opinión y de Expresión, citado en el informe de referencia, señaló que "*los avances tecnológicos entrañan que la eficacia de la vigilancia realizada por el Estado ya no se vea limitada por su magnitud o duración*".[83]

81 Asamblea General de las Naciones Unidas. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. La vigilancia y los derechos humanos. 28 de mayo de 2019, párr.29.

82 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Informe: El Derecho a la privacidad en la era digital, párr. 2.

83 Asamblea General de las Naciones Unidas. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad

181. De lo expuesto, se advierte que el surgimiento de nuevas tecnologías para la vigilancia, intervención y recolección de datos ha abierto la puerta para la práctica de injerencias a la vida privada que pudieran ser arbitrarias e ilegales por las causas estrechamente interrelacionadas que se abordan en la presente Recomendación General: la primera consiste en la existencia de marcos regulatorios deficientes relativos a la intervención de comunicaciones; la segunda, es el fortalecimiento de las facultades discrecionales de los órganos de inteligencia y de las autoridades de procuración de justicia para realizar actos de vigilancia mediante el uso de cualquier clase de tecnología, derivado de la ausencia de mecanismos y controles efectivos por órganos independientes; la tercera, es la ausencia absoluta de regulación sobre el tipo y alcances de tecnologías que pueden ser adquiridas y utilizadas en la intervención de comunicaciones, y la cuarta, es la adquisición de tecnologías de vigilancia que a pesar de que por sus características pudieran rebasar los fines constitucionalmente permitidos, se utilizan bajo esquemas legales que no corresponden a su potencialidad lesiva creando con ello un riesgo grave.

C. DEBER DE PREVENCIÓN DEL ESTADO MEXICANO

182. El grave riesgo que enfrenta la sociedad mexicana y, dadas las circunstancias particulares ya expuestas, los periodistas, comunicadores y personas defensoras de derechos humanos al haberse acreditado que, entre 2011 y 2017, diversas instituciones del Estado mexicano adquirieron Pegasus, omitiendo tomar las medidas necesarias para contener el riesgo asociado a la posesión y uso de un sistema con una alta potencialidad lesiva de derechos humanos debido a sus capacidades y alcances; lo cual se vincula al incumplimiento del deber institucional de prevención que emana del derecho humano a la seguridad jurídica, acorde a los razonamientos que se exponen a continuación.[84]

de opinión y expresión. A/HCR/23/40, párr. 33.

84 La CrIDH ha señalado sobre el "deber de prevención", que la obligación de garantizar los derechos humanos presupone el deber de los Estados de prevenir que esto sean violentado. El deber de prevención "[…] *abarca todas aquellas medidas de carácter jurídico, político, administrativo y cultural que promuevan la salvaguarda de los derechos humanos y que aseguren que las*

183. El artículo 1 de la Convención Americana establece la obligación de todos los Estados parte de respetar los derechos y libertades reconocidos en ella y garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción. Así mismo, el artículo 2 establece: "*Si el ejercicio de los derechos y libertades mencionados en el artículo 1 no estuviere ya garantizado por disposiciones legislativas o de otro carácter, los Estados Parte se comprometen a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones de esta Convención, las medidas legislativas o de otro carácter que fueren necesarias para hacer efectivos tales derechos y libertades*".

184. Con base en los artículos señalados, los Estados Parte deben asumir los deberes fundamentales de respeto y de garantía, por lo cual todo menoscabo a los derechos humanos reconocidos en la Convención que pueda ser atribuido, según las reglas del derecho internacional, a la acción u omisión de cualquier autoridad pública, constituye un hecho imputable al Estado que compromete su responsabilidad en los términos previstos por la misma Convención.

185. La CrIDH ha señalado al respecto, que la primera obligación asumida por los Estados Partes, en los términos del citado artículo, es "respetar los derechos y libertades" reconocidos en la Convención y que la segunda obligación es "garantizar" el libre y pleno ejercicio de los derechos reconocidos en la Convención a toda persona sujeta a su jurisdicción, la cual implica "*el deber (…) de organizar todo el aparato gubernamental y, en general, todas las estructuras a través de las cuales se manifiesta el ejercicio del poder público, de manera tal que sean capaces de asegurar jurídicamente el libre y pleno ejercicio de los derechos humanos.*"[85]

eventuales violaciones a los mismos sean efectivamente consideradas y tratadas como un hecho ilícito que, como tal, es susceptible de acarrear sanciones para quien las cometa, así como la obligación de indemnizar a las víctimas por sus consecuencias perjudiciales. Es claro, a su vez, que la obligación de prevenir es de medio o comportamiento y no se demuestra su incumplimiento por el mero hecho de que un derecho haya sido violado." *Caso Defensor de Derechos Humanos y otros Vs. Guatemala*". Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de agosto de 2014, párr. 139.

85 *Caso Velásquez Rodríguez Vs. Honduras*. Sentencia de Fondo 29 de julio de 1988, párr. 165 y 166.

186. Asimismo, la CrIDH ha señalado que la obligación de garantizar el libre y pleno ejercicio de los derechos humanos no se agota con un orden normativo dirigido a hacer posible el cumplimiento de esta obligación, sino que comparta la necesidad de una conducta gubernamental que asegure en la realidad una eficaz garantía del libre y pleno ejercicio de los derechos humanos.

187. Aunado a lo anterior, la CrIDH ha subrayado que las infracciones a la Convención no pueden ser juzgadas aplicando reglas que tengan en cuenta elementos de naturaleza sicológica, orientados a calificar la culpabilidad individual de sus autores. "[…] *A los efectos del análisis, es irrelevante la intención o motivación del agente que materialmente haya violado los derechos reconocidos por la Convención, hasta el punto de que la infracción a la misma puede establecerse incluso si dicho agente no está individualmente identificado. Lo decisivo es dilucidar si una determinada violación a los derechos humanos reconocidos por la Convención ha tenido lugar con el apoyo o la tolerancia del poder público o si éste ha actuado de manera que la trasgresión se haya cumplido en defecto de toda prevención o impunemente. En definitiva, de lo que se trata es de determinar si la violación a los derechos humanos resulta de la inobservancia por parte de un Estado de sus deberes de respetar y de garantizar dichos derechos, que le impone el artículo 1.1 de la Convención"*.[86]

188. De la información obtenida por este Organismo Nacional, se acreditó que diversas instituciones del Estado mexicano, entre 2011 y 2017, adquirieron la licencia de uso y explotación de Pegasus.

189. No obstante lo anterior, las instituciones del Estado mexicano no proporcionaron información o constancias de las que se adviertan criterios, lineamientos, directrices, acuerdos, manuales o disposición alguna en la que se especificara con claridad cuál era el procedimiento y/o protocolos para el uso de Pegasus, quiénes y cuál era el perfil de

86 *Ibidem*, párr.173.

las personas servidoras públicas responsables de su empleo y del manejo de la información obtenida, cuántos de ellos poseían las claves para su manejo, cuáles eran sus facultades, responsabilidades y límites en el ejercicio de sus atribuciones con respecto al resguardo y uso de dicho sistema, así como el manejo y resguardo de la información que pudiera ser obtenida a través de éste, cuáles eran las limitaciones en el uso de ese sistema, las salvaguardas a los derechos humanos en su utilización, y los procedimientos o medios de supervisión que vincularan a las empresas privadas responsables del desarrollo de tal sistema y de su comercialización.

190. Sobre el particular, este Organismo Nacional reitera que la FEADLE deberá realizar una investigación exhaustiva para acreditar la responsabilidad de todas las personas servidoras públicas y terceros involucrados en el caso.

191. La CrIDH ha establecido que constituye un hecho ilícito aquél que es violatorio de derechos humanos, lo cual puede acarrear la responsabilidad internacional del Estado, no por el hecho en sí mismo, sino por falta de la debida diligencia para prevenir la violación o para tratarla en los términos requeridos por la Convención.

192. El deber de prevención abarca todas aquellas medidas de carácter jurídico, político, administrativo y cultural que promuevan la salvaguarda de los derechos humanos y que aseguren que las eventuales violaciones a los mismos sean efectivamente consideradas y tratadas como un hecho ilícito que, como tal, es susceptible de acarrear sanciones para quien las cometa.[87]

193. En el caso particular, las instituciones de la administración pública que adquirieron Pegasus entre 2011 y 2017, forman parte de la estructura constitucional del Estado mexicano, el cual tiene la obligación de observar y respetar los derechos humanos acorde a lo establecido en la Convención y en el artículo 1° de la Constitución Política

87 *Caso Velásquez Rodríguez Vs. Honduras*, párr.175.

de los Estados Unidos Mexicanos; ello implica el deber de conocer e incorporar en su orden normativo los estándares internacionales sobre derechos humanos que resultan, entre otras fuentes, de los pronunciamientos realizados por diversas entidades y organismos internacionales especializados.

194. Tal es el caso de los pronunciamientos que han hecho la Relatoría Especial para la Libertad de Expresión de la CIDH, y la Relatoría Especial para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión de las Naciones Unidas, las cuales, tanto en Informes Anuales como en Declaraciones conjuntas e Informes Especiales, han abordado la problemática originada por la inadecuada regulación sobre la adquisición y uso de tecnologías para la intervención de comunicaciones.

195. Lo anterior implica que las instituciones del Estado mexicano, en atención a las observaciones y recomendaciones realizadas por los Relatores Especiales, aun antes de adquirir la licencia para uso y explotación de Pegasus y, con mayor razón, una vez que éste les fue físicamente entregado para su operación, debieron tomar las medidas necesarias y pertinentes, en cumplimiento a su deber de cuidado, para evaluar, gestionar y mitigar el riesgo que la adquisición, posesión y posible uso de Pegasus representa, ya que es un sistema que propicia las violaciones a derechos humanos.

196. Para ello, debieron transparentar el proceso de adquisición de tal sistema, y establecer con claridad, ya sea a través de criterios, lineamientos, directrices, manuales, acuerdos o documento diverso, cuál era el procedimiento y/o protocolos para el uso de Pegasus, quienes y cuál era el perfil de las personas servidoras públicas responsables de su empleo y del manejo de la información obtenida, cuántos de ellos poseían las claves para su manejo, cuáles eran sus facultades, responsabilidades y límites en el ejercicio de sus atribuciones con respecto al resguardo y uso de dicho sistema, cuáles eran las limitaciones en el uso de ese sistema, las salvaguardas a los derechos humanos en la utilización del sistema, los procedimientos o medios de supervisión que además

vincularan a las empresas privadas responsables del desarrollo de tal sistema y de su comercialización.

197. Adicionalmente, debieron transparentar el uso y el alcance de las técnicas y atribuciones de vigilancia de las comunicaciones. Además, atendiendo a la recomendación del Relator Especial, debieron considerar en tales disposiciones normativas publicar periódicamente información completa sobre el número de solicitudes aprobadas y rechazadas y un desglose de las solicitudes por investigación y propósito.[88]

198. Sin embargo, las instituciones del gobierno mexicano que adquirieron Pegasus ignoraron dichos pronunciamientos, ya que no emitieron disposición alguna a través de los cuales incorporaran los criterios señalados, por lo que se advierte una falta de voluntad para atender la problemática que implicaba el riesgo por la adquisición, posesión y posible uso de Pegasus, incumpliendo con ello, el deber de prevención que se vincula al derecho humano a la seguridad jurídica en agravio de toda persona que se encuentre en territorio nacional, especialmente de periodistas y personas defensoras de derechos humanos.

199. Sobre el particular, destaca el criterio de la CrIDH en el que se establece que si el aparato del Estado actúa de modo que las violaciones queden impunes y no se restablezca, en cuanto sea posible, a las víctimas en la plenitud de sus derechos, puede afirmarse que ha incumplido el deber de garantizar su libre y pleno ejercicio a las personas sujetas a su jurisdicción. Lo mismo es válido cuando se tolere que los particulares o grupos actúen libre o impunemente en menoscabo de los derechos humanos reconocidos en la Convención.[89]

200. En concordancia con los pronunciamientos de la CrIDH, este Organismo Nacional considera que la problemática advertida también se vincula a la participación de las

88 Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, párr. 91.
89 *Caso Velásquez Rodríguez vs. Honduras*, párr.176.

empresas privadas en el desarrollo y comercialización de los sistemas para la intervención de comunicaciones privadas, por la ausencia de regulación que vincule de manera clara, directa y específica, su responsabilidad por las violaciones a derechos humanos que resulten del uso de tales tecnologías, ni siquiera a nivel contractual.

201. El Relator Especial sobre la Promoción y Protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas, en el informe publicado en 2019, titulado: "La vigilancia y los Derechos Humanos", ha advertido que los gobiernos y el sector privado colaboran estrechamente en el mercado de los instrumentos para la vigilancia digital, "[a]*unque se desconoce si las empresas llevan a cabo algún tipo de diligencia para evaluar la trayectoria de los compradores en materia de derechos humanos*".[90]

202. El informe reconoce que si bien "[…] *puede ser que las empresas pretendan de manera genuina que sus productos se utilicen para una 'interceptación legal' por parte de las autoridades públicas autorizadas contra objetivos legítimos, con la autorización de las autoridades judiciales u otras autoridades independientes […], eso no se puede saber con certeza porque todos los aspectos de esa colaboración –desde la debida diligencia y las ventas hasta el apoyo al usuario final– suelen llevarse a cabo con una supervisión y una transparencia limitadas. […]"*[91]

203. En el mismo tenor, el Relator destaca que el riesgo extraordinario del mal uso de los productos de vigilancia significa que las empresas deben anticipar el uso ilícito de sus programas y comenzar a diseñar soluciones para reparar los inevitables impactos negativos. Sin embargo, también puntualiza que no hay ninguna información pública que sugiera que las evaluaciones desde la óptica de los derechos humanos sean un componente habitual de los procesos de diligencia debida durante las ventas, ni que esas

90 28 de mayo de 2019, párr. 15.
91 *Ibidem*, párr. 16.

evaluaciones se mantengan a lo largo del ciclo de vida del producto y del contrato de servicios posventa.[92]

204. Bajo ese panorama, las instituciones de la administración pública que adquirieron sistemas de tal naturaleza entre 2011 y 2017, tenían un deber reforzado de prevención, en tanto su obligación constitucional como instituciones que forman parte del Estado mexicano para la protección y defensa de los derechos humanos de todas las personas bajo su jurisdicción, por lo que debieron asegurarse que en los contratos que suscribieron con empresas privadas, relativos a la adquisición y transferencia de tales tecnologías, se establecieran las salvaguardas necesarias y adecuadas para la protección de derechos humanos, además de estipular las responsabilidades que deben asumir las empresas desarrolladoras y comercializadoras de tales sistemas.

205. Entre las medidas que inequívocamente deben ser establecidas en los contratos suscritos por los Estados y las empresas responsables del desarrollo, venta y distribución de dichos sistemas, se encuentran las señaladas por el Relator Especial, entre las que destacan las siguientes: señalamiento de la responsabilidad de las empresas de respetar la libertad de expresión, la privacidad y los derechos humanos en todas las operaciones, cumplimiento del derecho internacional de los derechos humanos por las partes como condición para la aprobación y conclusión de la venta, transferencia, y la prestación de servicios de asistencia; establecimiento de prohibiciones claras y específicas sobre la modificación personalizada de los productos, la selección de objetivos y la prestación de servicios de mantenimiento o asistencia que supongan una infracción al derecho internacional de los derechos humanos; establecimiento de procesos internos que garanticen que en las opciones de diseño e ingeniería se incorporen salvaguardias de los derechos humanos, como pueden ser sistemas de aviso que detecten el uso indebido e interruptores que puedan activarse en esos casos, entre otras.[93]

92 *Ibidem*, párrafos. 32 y 33.

93 *Ibidem*, párr. 60.

206. No obstante, de la información con que cuenta este Organismo Nacional se advierte que las diversas instituciones del Gobierno mexicano al suscribir los contratos con las empresas vinculadas a la empresa desarrolladora de Pegasus, no consideraron salvaguardas para la protección y defensa de derechos humanos a pesar del riesgo manifiesto que un sistema como ese involucra, acorde a los informes publicados por los Relatores Especiales de la OEA y ONU anteriormente citados.

207. En mérito de lo expuesto, el Gobierno de México incumplió con el deber de prevención[94], derivado de su omisión, ya que a pesar de haber tenido pleno conocimiento de que diversas instituciones de la administración pública efectivamente adquirieron Pegasus entre 2011 y 2017, en ningún caso se consideraron las salvaguardas para la debida protección y defensa de derechos humanos, a pesar de tratarse de un sistema tecnológico con alta potencialidad lesiva.

D. RIESGO REAL DE VIOLACIÓN A LOS DERECHOS HUMANOS A LA LIBERTAD DE EXPRESIÓN Y EL DERECHO A DEFENDER POR EL USO DE TECNOLOGÍAS EN PODER DE INSTITUCIONES DEL ESTADO MEXICANO PARA LA VIGILANCIA, INTERVENCIÓN Y RECOLECCIÓN DE DATOS

208. Este Organismo Nacional advierte la posibilidad de afectaciones a los derechos humanos a la Libertad de Expresión y el Derecho a Defender, a través de un medio indirecto constituido por el efecto amedrentador y la autocensura de periodistas y

94 El deber de prevención implica "a) el desarrollo de todas aquellas medidas de carácter jurídico, político, administrativo y cultural que promuevan la salvaguarda de derechos humanos para que tanto en la ley como en la práctica se asegure que las eventuales violaciones a los mismos sean efectivamente consideradas y tratadas como un hecho ilícito, que es susceptible de acarrear sanciones, capaz de contrarrestar y combatir los factores de riesgo; b) la aplicación de medidas tendientes al logro de metas a largo plazo con la finalidad de generar conciencia acerca de la importancia de los derechos humanos y el papel fundamental que juega su materialización en la construcción de una sociedad incluyente, solidaria y participativa cuyos efectos podrá definirse sólo a largo plazo; c) el deber del Estado de asegurar que las personas bajo su jurisdicción no sufran violaciones por parte de terceros o incluso de autoridades a través de la adopción de disposiciones normativas u otro tipo de medidas; d) la conducta del Estado para abstenerse de realizar acciones directas que signifiquen la transgresión de las violaciones a los derechos humanos de las personas que habitan y transitan en el Estado". Cuadernillo "*Deberes específicos de prevención, investigación y sanción*". Coeditado por SCJN-Oficina en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH)-Comisión de Derechos Humanos del Distrito Federal (CDHDF). Primera edición, 2013. México; pág. 60.

personas defensoras de derechos humanos, ante el riesgo de ser objeto de actos de vigilancia mediante el uso de sistemas cuyo marco regulatorio permite su empleo discrecional y secreto, circunstancias en las que se abunda en los siguientes apartados.

D.1. Libertad de expresión

209. La libertad de expresión está reconocida en el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, en cuyos párrafos primero y segundo se establece lo siguiente: "*La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, a la vida privada o los derechos de terceros, provoque algún delito o perturbe el orden público, el derecho de réplica será ejercido en los términos dispuestos por la Ley. El derecho a la información será garantizado por el Estado. Toda persona tiene derecho al libre acceso a la información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión*".

210. En tanto que, el artículo 7º, párrafo primero, de la Constitución Política de los Estados Unidos Mexicanos señala: "*Es inviolable la libertad de difundir opiniones, información e ideas a través de cualquier medio. No se puede restringir este derecho por vías o medios indirectos* […]".

211. En el mismo tenor, la Convención Americana sobre Derechos Humanos establece en su artículo 13, numerales 1 y 3, que: "*1. Toda persona tiene derecho a la libertad de pensamiento y expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección"* […]. *3. No se puede restringir el derecho de expresión por vías o medios*

indirectos, […] *por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones"*.

212. Al respecto, la Declaración de Principios sobre Libertad de Expresión, en los puntos 1°, 4°, 5°, 6°, 7° y 9°, advierte la relevancia de la libertad de prensa para la realización del pleno y efectivo ejercicio de la libertad de expresión y como instrumento indispensable para el funcionamiento de la democracia representativa, y subraya que la libertad de expresión no es una concesión del Estado, sino un derecho humano mediante el cual los ciudadanos ejercen su derecho a recibir, difundir y buscar información, por lo que la censura previa, interferencia o presión directa o indirecta sobre cualquier expresión, opinión o información difundida, debe estar prohibida.

213. La Relatoría para la Libertad de Expresión de la CIDH ha señalado que el respeto y protección de la libertad de expresión adquiere una función primordial, ya que sin ella es imposible que se desarrollen todos los elementos para el fortalecimiento democrático y el respeto a los derechos humanos. "*El derecho y respeto de la libertad de expresión se erige como instrumento que permite el intercambio libre de ideas y funciona como ente fortalecedor de los procesos democráticos, a la vez que da, otorga a la ciudadanía una herramienta básica de participación. Asimismo, a través de los comunicadores sociales, la ciudadanía adquiere el poder de participar y/o controlar el desempeño de las acciones de los funcionarios públicos.*"[95]

214. Igualmente, la CrIDH, en la Opinión Consultiva OC-5/85 señaló que: "*[L]a libertad de expresión es una piedra angular en la existencia misma de una sociedad democrática. Es indispensable para la formación de la opinión pública (…) para que la comunidad, a la hora de ejercer sus opciones, esté suficientemente informada. Por ende, es posible afirmar que una sociedad que no está bien informada no es plenamente libre".* La libertad de expresión es por lo tanto, no sólo un derecho de los individuos sino de la sociedad misma.[96]

95 OEA. "Antecedentes e Interpretación de la Declaración de Principios sobre la Libertad de Expresión", Principio 1, párr. 7.
96 "Colegiación Obligatoria de Periodistas", del 13 de noviembre de 1985, solicitada por Costa Rica, párr. 70.

215. De lo anterior se advierte que dada la relevancia de la libertad de expresión y prensa, tanto la Constitución Política de los Estados Unidos Mexicanos, como la Convención Americana sobre Derechos Humanos e instrumentos que incorporan estándares internacionales, reconocen la prohibición expresa del empleo de medios indirectos para lograr coartar tales derechos.

216. Resulta necesario distinguir entre un medio directo de censura de la libertad de expresión de uno indirecto, con la finalidad de identificar la razón por la cual la afectación a este derecho humano deriva precisamente del uso de medios indirectos.

217. La Relatoría para la Libertad de Expresión de la CIDH, advierte que con frecuencia se configuran conductas que a lo largo del tiempo se han considerado formas "típicas" de violación a este derecho. Esto implica que esas medidas han sido concebidas expresamente para "silenciar" el ejercicio de la libertad de expresión, entre las más frecuentes se encuentran las amenazas, hostigamiento, desapariciones y, la más grave de todas, el homicidio.[97]

218. Respecto a los medios indirectos, la misma Relatoría refiere que "*existen formas indirectas más sutiles y a veces más efectivas por las que el Estado coarta la libertad de expresión. Debido a que estas violaciones indirectas son con frecuencia obstrucciones oscuras, impuestas silenciosamente, no dan lugar a investigaciones ni merecen una censura generalizada, como ocurre con otras violaciones más directas*".[98]

219. Dichas medidas, a diferencia de las anteriores, no han sido diseñadas estrictamente para restringir la libertad de expresión. "[…] éstas *per se* no configuran una violación de este derecho. No obstante ello, sus efectos generan un impacto adverso en la libre

97 Violaciones Indirectas de la Libertad de Expresión: Asignación Discriminatoria de la Publicidad Oficial, 2003, Capítulo V, pp. 187-209.
98 *Ibidem,* Introducción, pág. 1.

circulación de ideas que con frecuencia es poco investigado y, por ende, más difícil de descubrir".[99]

220. Como ha sido expuesto, esta Comisión Nacional cuenta con información de la que se acredita que, entre 2011 y 2017, diversas instituciones del Estado mexicano adquirieron tecnologías para la vigilancia, intervención y recolección de datos. También se acredita que tanto las adquisiciones de dichas tecnologías, como su posible uso se regulan mediante esquemas legales que no corresponden a su potencialidad lesiva que, aunado a ello, no hay mecanismos y controles efectivos por órganos independientes que aseguren que su posible utilización no rebase los fines constitucionalmente establecidos y que además, las normas que regulan la intervención de comunicaciones privadas dotan de facultades discrecionales a las autoridades de inteligencia e investigadoras de delitos.

221. Aunado a lo anterior, se advierte que durante 2015 y 2016, personas periodistas y defensoras de derechos humanos recibieron mensajes de texto con enlaces maliciosos en sus teléfonos celulares que, de acuerdo al estudio realizado por **O1**, constituían intentos de infección vinculados a Pegasus, destacando el hecho de que el periodo de recepción de tales mensajes coincide con aquel durante el cual las Instituciones del Gobierno del Estado mexicano adquirieron Pegasus.

222. El contexto descrito, aunado a la falta de certeza respecto de la regulación y controles evidencia la posible inhibición en el ejercicio del derecho a la libertad de expresión, al producirse un efecto intimidatorio y, en consecuencia, de silenciamiento con un alto impacto en las personas periodistas y comunicadoras.

D.2. Derecho a defender Derechos Humanos

223. El artículo 1º de la "Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos", indica que: "*toda persona tiene derecho*

99 *Ibidem*. Primera parte: cuestiones básicas. Violaciones directas e indirectas a la libertad de expresión. párr. 9.

individual o colectivamente a promover y procurar la protección y realización de los derechos humanos y las libertades fundamentales en los planos nacional e internacional".[100]

224. En atención a ese artículo, la Comisión Interamericana de Derechos Humanos ha señalado que debe ser considerado defensor o defensora de derechos humanos: "*toda persona que de cualquier forma promueva o procure la realización de los derechos humanos y las libertades fundamentales reconocidos a nivel nacional o internacional".*[101]

225. La Ley para la Protección de Personas Defensoras de Derechos Humanos y Periodistas, en su artículo 2, señala que serán consideradas como personas defensoras de derechos humanos todas aquéllas "*que actúen individualmente o como integrantes de un grupo, organización o movimiento social, así como personas morales, grupos, organizaciones o movimientos sociales cuya finalidad sea la promoción o defensa de los derechos humanos*".

226. Tal y como se señala en la Recomendación General 25, "Sobre agravios a personas defensoras de derechos humanos", la relevante labor que desempeñan las personas defensoras de derechos humanos ha sido puesta de relieve en distintos documentos, así como por diversos organismos y tribunales internacionales. La CIDH ha expresado su reconocimiento por el admirable trabajo que realizan para dar efectividad a los derechos humanos de los habitantes de la región americana. Reconoce que este grupo de individuos y organizaciones son el enlace entre la sociedad civil en el plano interno y el sistema de protección de los derechos humanos en el ámbito internacional, por lo que su papel en la sociedad es fundamental para garantizar y salvaguardar la democracia y el Estado de derecho.[102]

100 Aprobada por la Asamblea General de la ONU mediante resolución A/RES/53/144 de 9 de diciembre de 1998, art. 1.
101 Informe sobre la Situación de las Defensoras y Defensores de los Derechos Humanos en las Américas, 2006, párr. 13.
102 Informe sobre la Situación de las Defensoras y los Defensores..., *Óp. Cit.*, párr. 332, p. 59. CNDH, citado en la Recomendación General 24, de 8 de febrero de 2016, párr. 8.

227. Lamentablemente su propia labor ha ocasionado que sean blanco de diversas agresiones, empleando para ello tanto medios directos como indirectos, cuya naturaleza ha sido precisada en párrafos precedentes. Al respecto, los Relatores Especiales de la ONU y OEA han advertido que la vigilancia selectiva *"[…] crea incentivos para la autocensura y menoscaba de manera directa la capacidad de los periodistas y los defensores de derechos humanos para realizar investigaciones y para forjar y mantener relaciones con fuentes de información".*[103] En el mismo sentido el Comité de Derechos Humanos ha señalado que *"[…] las restricciones nunca se pueden hacer valer como justificación para silenciar a los defensores de la democracia pluripartidista, los principios democráticos y los derechos humanos*."[104]

228. El mismo efecto de silenciamiento del que pueden ser víctimas las y los periodistas y comunicadores, se verifica en las personas defensoras de derechos humanos, ante el riesgo de ser objeto de actos de espionaje mediante el uso de sistemas para la intervención de sus comunicaciones, con lo que la labor que realizan de representación y defensa de otros grupos en situación de riesgo se podría ver seriamente afectada, en perjuicio de la sociedad.

229. Se afirma lo anterior, ya que si bien el uso de tecnologías para la información y comunicación son herramientas indispensables para facilitar la labor que desarrollan las personas defensoras de derechos humanos, puesto que a través del uso de redes sociales, mensajes electrónicos, video y audioconferencias, entre otras, les es posible llegar rápidamente a muchas personas, realizar llamados sobre acciones urgentes, difundir peticiones en línea, promover acciones que generen conciencia, además de facilitar el contacto entre las mismas personas defensoras; ante el contexto descrito en la presente Recomendación, dichas herramientas involucran una vulnerabilidad y un riesgo derivado de su posible intervención mediante el uso de sistemas semejantes a Pegasus.

103 Informe Especial sobre la Situación de la Libertad de Expresión en México. 2018, párr. 53.
104 Observación General 34 (2011) *"Sobre la libertad de opinión y de expresión"*, párr. 23

230. Personas defensoras han reconocido que activistas alrededor del mundo evitan utilizar llamadas telefónicas y mensajes de texto tradicionales ante el riesgo de ser monitoreados, sin embargo, son susceptibles de ser objeto de actos de espionaje a través de sus comunicaciones por medio de internet, como el correo electrónico, llamadas de voz sobre IP o mensajería instantánea[105], lo que preocupa sensiblemente, ya que debido a las actividades de defensa que realizan enfrentan una situación de riesgo mayor.

231. En efecto, la posición de las personas defensoras de derechos humanos las coloca como un sector en riesgo, debido a la sobreexposición a las agresiones y a otras violaciones a sus derechos humanos, tanto por las personas servidoras públicas como por particulares; por ello, es necesario analizar los contextos social, político y económico que se interrelacionan con su labor, en función de los grupos en situación de vulnerabilidad a los que representan.

232. En la citada Recomendación General 25, este Organismo Nacional señaló que toda agresión a las personas defensoras de derechos humanos, ya sea por medios directos o indirectos, adquiere una real importancia en la problemática social, en razón de que lesiona de manera sensible, en general, a la población y, particularmente, a este grupo de personas, ya que por cada persona defensora que ve limitada, afectada o anulada su labor con motivo de agresiones como la criminalización o estigmatización, otras más en situación de riesgo, como es el caso de mujeres, pueblos indígenas, personas migrantes, niños y niñas, personas mayores, personas con VIH/SIDA, y de la comunidad LGBTTTI, por ejemplo, que son representados y defendidos por dichos defensores, se ven afectados al encontrarse expuestos en un medio en el que se les priva de manera directa

105 Rogelio López Aguilar, "*Desarrollo de diferentes tecnologías para el ejercicio y defensa de los derechos en internet (software libre)*", publicado en *Revista de Derechos Humanos Defensor*. CDHDF; junio, 2016. Pp. 32-33.

o indirecta de la labor de quienes han asumido los riesgos de constituirse en su voz, en la lucha por el respeto a sus derechos fundamentales.

233. Lo anterior es así, en virtud de que el derecho a defender se ejerce respecto de las personas físicas, morales, comunidades, grupos sociales o colectivos que históricamente han padecido discriminación, exclusión, condiciones de marginación y/o pobreza, entre otras, por lo que parte fundamental de la labor de las personas defensoras es la denuncia social, en busca de mejores condiciones tanto sociales como políticas o económicas para los más desfavorecidos.[106]

234. Las actividades desarrolladas por las personas defensoras de derechos humanos, frecuentemente se relacionan con la investigación, denuncia y seguimiento de temáticas sensibles y de interés público, lo actualizan la presunción sobre el riesgo de que sean objeto de actos de espionaje mediante el uso de las tecnologías descritas, lo cual basta para generar el efecto amedrentador al que se ha aludido en párrafos precedentes y, en consecuencia, pudiere tener como efecto la autocensura, limitando con ello la labor que realizan, con lo que se actualiza la violación al derecho humano a defender.

235. Al tenor de lo expuesto, la CNDH identifica una sensible problemática que deriva del hecho plenamente probado de que autoridades del gobierno federal adquirieron Pegasus en el periodo de 2011 a 2017, que a pesar de la potencialidad lesiva de dicho sistema, no tomaron medida alguna que les permitiera contener el riesgo y prevenir las posibles violaciones a derechos humanos que su posesión y uso implica, ya que si bien existen disposiciones normativas relacionadas con la intervención de comunicaciones privadas, éstas son normas de carácter discrecional, cuya aplicación puede ser arbitraria, debido a que no incorporan disposiciones sobre el uso, alcances y límites de tecnologías para la vigilancia, intervención y recolección de datos.

236. En ese sentido, la CNDH advierte que es necesaria la participación de las diversas autoridades a quienes se dirige la presente Recomendación General para que, en el

106 CNDH. Recomendación General 25, "*Sobre agravios a personas defensoras de derechos humanos*". párr. 64.

ámbito de sus atribuciones, realicen las acciones para atender, resolver y prevenir la sensible problemática señalada, a través de las propuestas legislativas, reglamentarias y administrativas que correspondan.

237. Lo anterior sin perjuicio de que corresponderá al Ministerio Público de la Federación responsable de la integración de la CI, determinar la probable responsabilidad de las autoridades y terceros que pudieran estar involucradas en conductas constitutivas de delitos.

238. Sin perjuicio de lo expuesto en párrafos precedentes, cabe señalar que con motivo del análisis realizado por este Organismo Nacional se advirtió una falta de armonización legislativa entre la Ley Orgánica de la Administración Pública Federal y la Ley de Seguridad Nacional.

239. Lo anterior es así, ya que con motivo del "*Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Orgánica de la Administración Pública Federal*", publicado en el Diario Oficial de la Federación el 30 de noviembre de 2018, se creó la Secretaría de Seguridad y Protección Ciudadana, estableciendo sus facultades en el artículo 30 Bis de la Ley Orgánica en cita, en cuya fracción XVIII, se especifica su carácter como Secretaría Ejecutiva del Consejo de Seguridad Nacional. Antes de la referida reforma, la función de Secretaría Ejecutiva del Consejo de Seguridad Nacional correspondía a la Secretaría de Gobernación, según se advierte de la lectura del artículo 12, fracción II, de la vigente Ley de Seguridad Nacional.

240. Ahora bien, no obstante que el artículo Décimo Cuarto Transitorio del citado Decreto publicado el 30 de noviembre de 2018, prevé a la letra que: "*Las menciones contenidas en otras leyes, reglamentos y en general en cualquier disposición administrativa, a la Secretaría de Gobernación, en lo que se refiere a las facultades transferidas en virtud del presente Decreto a la Secretaría de Seguridad y Protección Ciudadana, se entenderán referidas a esta última*" (*sic*), esta Comisión Nacional considera necesario que el Congreso de la Unión realice los trabajos de armonización legislativa en relación a las disposiciones sobre el Consejo de Seguridad Nacional contenidas en la Ley de

Seguridad Nacional, a fin de que éstas sean acordes a la reforma de la Ley Orgánica de la Administración Pública Federal de 30 de noviembre de 2018 y al Reglamento de la citada Secretaría de Seguridad y Protección Ciudadana publicado en el Diario Oficial de la Federación el 30 de abril de 2019.

241. En el mismo tenor, la CNDH advierte que, si bien el artículo Octavo Transitorio del aludido Reglamento de la Secretaría de Seguridad y Protección Ciudadana, prevé que: "*Las menciones que en otras disposiciones se hagan al Centro de Investigación y Seguridad Nacional, se entenderán hechas al Centro Nacional de Inteligencia*", es necesario que se armonice el contenido de la citada Ley de Seguridad Nacional, que aún contempla en su Capítulo II, al extinto Centro de Investigación y Seguridad Nacional (CISEN).

242. Por otra parte y en consideración a que la Fiscalía General de la República, a la fecha de publicación de la presente Recomendación General, continúa la integración de la **CI,** en la cual, de acuerdo a información publicada en medios informativos[107], el 01 de noviembre de 2021, se cumplimentó una orden de aprehensión en contra de un probable responsable, este Organismo Nacional hace un llamado a la FEADLE para que, en respeto al derecho humano de acceso a la justicia, en su modalidad de procuración de justicia, realice las diligencias idóneas y necesarias para acreditar la responsabilidad de todas las personas servidoras públicas y terceros involucrados en el caso.

243. Lo anterior, en atención a que el artículo 17, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, establece el derecho de acceso a la justicia como la prerrogativa a favor de los gobernados de "acudir y promover ante las instituciones del estado competentes, la protección de la justicia a través de procesos que le permitan obtener una decisión en la que se resuelva de manera efectiva sobre sus pretensiones o derechos que estime le fueron violentados, en los plazos y términos

107 El título y localización de las publicaciones aludidas en el presente apartado se han resguardado en la hoja de claves, por tratarse de información que contiene datos personales que obran en fuentes públicas. Lo anterior de acuerdo con el Criterio 13/09 emitido por el INAI.

que fijen las leyes, emitiendo sus resoluciones de manera pronta, completa, imparcial y gratuita".

244. Así mismo, el artículo 116, fracción IX, de la Constitución Política de los Estados Unidos Mexicanos prevé que a nivel constitucional se debe garantizar que las funciones de procuración de justicia se realicen con base en los principios de autonomía, eficiencia, imparcialidad, legalidad, objetividad, profesionalismo, responsabilidad y respeto a los derechos humanos. En el mismo tenor, el artículo 16 del Código Nacional de Procedimientos Penales establece que toda persona tendrá derecho a ser juzgada dentro de los plazos legalmente establecidos y que las personas servidoras públicas de las instituciones de procuración e impartición de justicia deberán atender las solicitudes de las partes con prontitud, sin causar dilaciones injustificadas.

245. En el mismo sentido, el derecho a una adecuada administración de justicia se encuentra previsto en el artículo XVIII, de la Declaración Americana de los Derechos y Deberes del Hombre, artículo 6, inciso e), de la Declaración sobre Principios Fundamentales de Justicia para las Víctimas de Delitos y Abusos de Poder, así como artículo 14, del Pacto Internacional de Derechos Civiles y Políticos.

246. Por todos los argumentos expuestos, respetuosamente se formulan a ustedes: Comisión Bicamaral de Seguridad Nacional del Poder Legislativo; Cámara de Diputados y Cámara de Senadores del Congreso de la Unión; Secretaria de Seguridad y Protección Ciudadana en su calidad de Secretaria Ejecutiva del Consejo de Seguridad Nacional y, Fiscal General de la República; en el ámbito de sus competencias, las siguientes:

IV. RECOMENDACIONES GENERALES

A la Cámara de Senadores y a la Cámara de Diputados del Congreso de la Unión, así como a la Comisión Bicamaral de Seguridad Nacional del Poder Legislativo:

ÚNICO. Realicen las adiciones o modificaciones del marco jurídico actual sobre intervención de comunicaciones privadas, considerando los aspectos siguientes:

a. Se evite el uso de términos generales, abiertos y ambiguos, respecto a los actos que pueden ser considerados amenazas a la seguridad nacional, a fin de dar certeza jurídica a las personas quienes puedan ser objeto de acciones de vigilancia legal.

b. Se establezcan procedimientos que incorporen criterios claros e inequívocos sobre la elección, adquisición y uso de tecnologías para la vigilancia, intervención y recolección de datos, en los que se describan las restricciones para su uso y los medios de supervisión.

c. Se precise el perfil de las personas servidoras públicas responsables del uso de tecnologías para la vigilancia, intervención y recolección de datos, así como de las personas servidoras públicas responsables del manejo de la información obtenida mediante tales tecnologías, estableciendo de manera precisa sus facultades, responsabilidades y límites en el ejercicio de sus atribuciones.

d. Se prevea la responsabilidad de las empresas que desarrollen y comercialicen tales tecnologías, en aquellos casos en que sus actividades puedan ocasionar violaciones derechos humanos como consecuencia de las operaciones, productos o servicios que realicen.

e. Se incorpore de manera específica que, en los contratos suscritos con empresas responsables del desarrollo, venta y distribución de tecnologías para la vigilancia, intervención y recolección de datos, las partes contratantes se obliguen a respetar la libertad de expresión, la privacidad y los derechos humanos en todas las operaciones que desarrollen, en cumplimiento a las normas mexicanas y del derecho internacional del que el Estado mexicano sea parte, como condición para la aprobación de la venta, transferencia y la prestación de servicios de asistencia.

f. Se establezcan prohibiciones claras y específicas sobre la modificación personalizada de los productos, la selección de objetivos y la prestación de

servicios de mantenimiento o asistencia que supongan una infracción al derecho nacional o internacional de los derechos humanos.

g. Se establezca de manera específica que, en los contratos suscritos con empresas responsables del desarrollo, venta y distribución de tecnologías para la vigilancia, intervención y recolección de datos, se establezcan procesos internos que garanticen que en las opciones de diseño e ingeniería se incorporen acciones que permitan salvaguardar los derechos humanos, como pueden ser los sistemas de aviso, que detecten el uso indebido e interruptores que puedan activarse en tales casos.

h. Se incorporen criterios claros y específicos respecto a la aplicación de los principios de legalidad, necesidad, proporcionalidad e idoneidad en las solicitudes de intervención de comunicaciones, por motivos de seguridad nacional o investigación.

i. Se incorpore la obligación expresa a cargo del órgano de inteligencia, del Ministerio Público o bien, del Poder Judicial de la Federación, de notificar a la persona que fue objeto de actos de vigilancia por motivos de seguridad nacional o investigación de delitos, el periodo de tales injerencias, la totalidad de la información que fue obtenida, el uso y destino que se le dio.

j. Se realicen las adiciones o modificaciones al marco jurídico actual, para que se establezca como una obligación a cargo de las autoridades que realicen intervenciones a comunicaciones privadas, el rendir un informe al Poder Judicial de la Federación, con una periodicidad específica, sobre el uso y destino de los datos e información obtenidos, como estadístico.

A la Secretaría de Seguridad y Protección Ciudadana, en su calidad de Secretaria Ejecutiva del Consejo de Seguridad Nacional:

ÚNICO. Impulsar ante el Consejo de Seguridad Nacional la emisión de un instrumento administrativo (protocolo, lineamientos, criterios, manuales, directrices u acuerdos), mediante el cual se regule el uso de aparatos y/o sistemas útiles en la intervención de comunicaciones privadas que contenga los puntos siguientes:

- El procedimiento y los protocolos de seguridad para el uso de aparatos y/o sistemas útiles en la intervención de comunicaciones privadas, como Pegasus y otros análogos.

- Las limitaciones en el uso de aparatos y/o sistemas útiles en la intervención de comunicaciones privadas, como Pegasus u otros análogos, para salvaguardar los derechos humanos, precisando que sólo podrán ser utilizados cuando el marco normativo así lo establezca.

- Los procedimientos y medios de supervisión a cargo de una autoridad u órgano independiente respecto del uso de aparatos y/o sistemas útiles en la intervención de comunicaciones privadas.

- Responsabilidades de las empresas privadas desarrolladoras y comercializadoras de tal sistema y otros análogos.

A la Fiscalía General de la República:

ÚNICO. Se continúe con la integración de la **CI**, realizando las diligencias idóneas y necesarias para acreditar la responsabilidad de todas las personas servidoras públicas y terceros involucrados en dicha indagatoria.

247. La presente Recomendación es de carácter General, de acuerdo con lo señalado con los artículos: 102, apartado B, de la Constitución Política de los Estados Unidos Mexicanos; 6°, fracción VIII, de la Ley de la Comisión Nacional de los Derechos

Humanos, y 140 de su Reglamento Interno, habiéndose aprobado por el Consejo Consultivo de esta Comisión Nacional, en su sesión ordinaria número 406 de fecha 23 de mayo de 2022; tiene el carácter de pública y se emite con el propósito fundamental de que se promuevan los cambios y modificaciones de disposiciones normativas y prácticas administrativas que constituyen o propician violaciones a los derechos humanos, para que las autoridades competentes, dentro de sus atribuciones, eliminen dichas violaciones y subsanen las irregularidades de que se trate.

248. Con base en el mismo fundamento jurídico, se informa a ustedes que las Recomendaciones Generales no requieren de aceptación por parte de las instancias destinatarias. Sin embargo se requiere que, en su caso, las pruebas correspondientes al cumplimiento de las recomendaciones se envíen a esta Comisión Nacional en un término de treinta días hábiles siguientes a la fecha de emisión de la presente Recomendación.

PRESIDENTA

MTRA. MA. DEL ROSARIO PIEDRA IBARRA