**SÍNTESIS de la Recomendación General No. 47/2022, sobre la 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.
(DOF del 12 de diciembre de 2022)**

**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".**

**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.

**I. ANTECEDENTES**

**4.**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.

**5.**Con el objetivo de allegarse mayores datos relacionados con los hechos, este Organismo Nacional solicitó información a diversas autoridades.

**II. SITUACIÓN JURÍDICA**

**6.**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**

**7.**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 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.

**8.**Bajo esa tesitura, en la presente Recomendación General se aborda 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.

**9.**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.

**10.**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.

**11.**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.

**12.**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.

**13.**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**

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

**15.**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".

**16.**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.

**17.**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, que 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.

**B. MARCOS REGULATORIOS DEFICIENTES SOBRE LA INTERVENCIÓN DE COMUNICACIONES PRIVADAS**

**18.**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**

**19.**En México la intervención de comunicaciones(2)se encuentra prevista en el artículo 16, párrafos 12, 13 y 15, de la Constitución Política de los Estados Unidos Mexicanos, 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.

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

**21.**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.

**22.**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.

**23.**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.

**24.**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.

**25.**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.

**26.**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.(3)

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

**27.**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 de Seguridad Nacional, reflejan ambigüedad, ya que algunas de estas hipótesis pueden abarcarse por la legislación penal y otras no.(4)

**28.**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.

**29.**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**

**30.**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.

**31.**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.

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

**32.**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.

**33.**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.

**34.**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**

**35.**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.(5)

**36.**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.

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

**38.**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.

**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**

**39.**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 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**

**40.**La libertad de expresión está reconocida en el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, así como en la Convención Americana sobre Derechos Humanos establece en su artículo 13. 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.

**41.**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.

**42.**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**

**43.**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 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*".(6)

**44.**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.

**45.**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.

**46.**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.

**47.**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 Secretaría 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 Pegasusy otros análogos.

   Las limitaciones en el uso de aparatos y/o sistemas útiles en la intervención de comunicaciones privadas, como Pegasusu 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.

El texto íntegro de la Recomendación General No. 47/2022 puede ser consultado en la página de la CNDH, en la siguiente dirección electrónica: https://www.cndh.org.mx/sites/default/files/documentos/2022-05/RecGral\_47.pdf

El texto íntegro de la Recomendación General No. 47/2022, puede ser consultado en la página del DOF, en la siguiente dirección electrónica: https://www.dof.gob.mx/2022/CNDH/Sintesis-RecGral\_47.pdf

Atentamente

Ciudad de México, a 22 de noviembre de 2022.- Presidenta de la Comisión Nacional de los Derechos Humanos, Mtra. **Ma. del Rosario Piedra Ibarra**.- Rúbrica.

**(R.- 530209)**

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     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.

3     CIDH; 149 Periodo de Sesiones. Audiencia: Libertad de expresión y vigilancia de comunicaciones por parte de Estados Unidos; 28 de octubre de 2013.

4     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.

5     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 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.

6     Aprobada por la Asamblea General de la ONU mediante resolución A/RES/53/144 de 9 de diciembre de 1998, art. 1.