UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN

LA IMPORTANCIA DE LAS INSTITUCIONES POLÍTICAS EN LA REGULACIÓN DEL ESPIONAJE ELECTRÓNICO COMO UN DELITO DEL SIGLO XXI

T E S I S

QUE PARA OBTENER EL TÍTULO DE

L I C E N C I A D A E N R E L A C I O N E S I N T E R N A C I O N A L E S

P R E S E N T A:
RAQUEL RAMOS CRUZ

ASESOR:
MTRA. EN RELACIONES INTERNACIONALES
JUANA OTILIA MARTÍNEZ RAMÍREZ

Ciudad Nezahualcóyotl, Estado de México, Agosto de 2019

AGRADECIMIENTOS

A mi padre:

Luis Ramos Hernández por ser la máxima institución que reconozco, por ser el inquebrantable garante de mi seguridad, por ser el eterno defensor de mis derechos inclusive en contra de mi voluntad, por ser el gran ser humano a quien deseo imitar, por ser el hijo que llegó a una ciudad desconocida y se convirtió en un ejemplo para sus hermanos, por ser el padre que aceptó la total responsabilidad de educar a dos niñas, para un hombre como tú, sólo tengo un sentimiento y se llama: AMOR.

A mi madre:

Ernestina Cruz Torres por ser la mujer que me dio la vida, por enseñarme que del dolor se puede aprender, gracias a ello, elegí ser una mujer íntegra y determinada a conquistar todo aquello que le proporcione luz a mi alma.

A mi hermana:

Zitlali Ramos Cruz por ser la mujer más revolucionaria que conozco, porque aún no sé cómo logras hacer de una hazaña algo tan sencillo.

A mis sobrinos en paz descansen:

Alex y a ti que jamás conocí tu nombre por ser la luz que transformó a nuestra familia en seres humanos más conscientes y agradecidos con la vida. Quiero decirles que su mamá lo ha hecho extraordinariamente bien.

A mi hermano por elección:

Andrés de Jesús Morales Sánchez por ser quién eres, por ser un gran amigo, por tú autenticidad que me inspira a ser igual, tú eres y serás para mí, el mejor y el más talentoso artista.

A mis hermanas de carrera:

Monserrat Beltrán Cadena y Jazmín Martínez Villanueva por todos los momentos que hemos vivido, por no querer ser mis amigas y actualmente estas letras estén dedicadas a ustedes.

A mi asesora de tesis:

Mtra. Juana Otilia Martínez Ramírez por ser la guía que votó por mí cuando estaba a punto de rendirme, por ser más que una profesional admirable, por apoyarme a materializar un sueño que creía imposible. ¡Gracias desde el fondo de mi corazón!

A mi Universidad:

Por otorgarle a mi vida el obsequio más grande: un propósito.

Y por último para ti que estás leyendo:

Por ser el motivo de este trabajo, porque todo lo he hecho con el fin de que puedas leer este mensaje: ¡Por favor, no te rindas! ¡Lucha! ¡Es ahora o Nunca! No sé, cuán difícil puede ser para ti, pero sí sé que tienes una extraordinaria oportunidad en tus manos, recuerda que jamás volverás a ser tan joven, tan inteligente como lo eres ahora. Todos llevamos cicatrices en el alma pero somos más y mejores que eso. Sabes, desde aquí te imagino como él o la protagonista de un libro similar a los que hemos leído tanta veces, donde el héroe conquista sus sueños, encuentra el amor verdadero, sostiene entre sus brazos a sus hijos y cambia el curso de las generaciones. Y justo ese es mi deseo para ti. Te regalo el más cálido abrazo y sé que tú puedes.

Índice

INTRODUCCIÓN

El inicio del siglo XXI es un contexto marcado por los ataques terroristas del 11 de Septiembre en Estados Unidos. Los acontecimientos subsecuentes como: la guerra de Afganistán (2001), la guerra de Irak (2003), la crisis económica (2008), la Primavera Árabe (2010-2013), las revelaciones sobre la red de vigilancia mundial (2013-2015), los atentados de París (2015), los atentados de Bruselas (2016), los atentados de Berlín (2016), son el resultado de una guerra emprendida por el gobierno estadounidense contra el terrorismo.

Simultáneamente, las tecnologías de la información y comunicación revolucionaron nuestra forma de percibir el mundo. El desarrollo, la digitalización y el control de la información a nivel global, mediante nuevos dispositivos de almacenamiento de datos, la expansión de la telefonía móvil y las redes sociales generaron nuevas actividades y con ellas la existencia de nuevos delitos en el ciberespacio.

Entre 2013 y 2015, la prensa internacional hizo de conocimiento público el contenido de documentos confidenciales, propiedad de la Agencia de Seguridad Nacional de Estados Unidos: se constató que la agencia de inteligencia estadounidense, en colaboración con las agencias de inteligencia de otros países aliados (el Mossad, el MI5, el MI6, el Cuartel General de Comunicaciones del Gobierno británico) y las más importantes empresas de telecomunicaciones, tecnología e Internet (Microsoft, Google, Apple, Facebook, Yahoo!, AOL, Verizon, Vodafone, Global Crossing o British Telecommunications, entre otras), han estado ejerciendo una vigilancia masiva sobre la población mundial.

Es decir, los gobiernos para garantizar la seguridad nacional hacen uso de la tecnología, al desarrollar herramientas sofisticadas de vigilancia electrónica (espionaje electrónico o ciberespionaje). Programas diseñados para obtener información de ciudadanos nacionales y extranjeros. Es así que, vulneran la privacidad de la población mundial, al incluir entre sus objetivos a todo individuo que, no es sospechoso de cometer ningún delito.

Es verdad que los estados requieren de todos los medios disponibles para garantizar su supervivencia. El problema reside cuando la tecnología se utiliza sin controles ni objetivos específicos, cuando es aplicada a grupos y personas que manifiestan estar en desacuerdo con el poder político de sus gobiernos, y en su búsqueda de evitar la censura se vuelcan a los medios en línea, en donde son monitoreados, denigrados públicamente o arrestados. Medidas aplicadas por algunos gobiernos (Turquía, Egipto, Vietnam, Arabia Saudita, China, Chechenia, Omán), que han establecido, para los delitos de expresión en línea, penas más severas que las previstas para delitos equivalentes fuera de línea. Es por eso que el ciberespionaje es una amenaza para la privacidad. Un derecho esencial para la dignidad humana y primordial en una sociedad democrática. Por tal razón, su restricción sólo puede estar justificada cuando es prescrita por la ley, es necesaria para lograr un objetivo legítimo y es proporcional al objetivo perseguido.

En los años recientes, el Estado Mexicano fue víctima del “Grupo Equation”, responsable del espionaje electrónico global que atacó la infraestructura informática de más de treinta países, con el apoyo de la Agencia de Seguridad Nacional estadounidense. En México se detectó un nivel "medio de infección" de estas herramientas, principalmente en los sectores de gobierno y financiero, aunque se desconoce el impacto de esta campaña de ataques cibernéticos en contra de la infraestructura de gobierno.

Por otra parte, el informe “Gobierno Espía: La vigilancia sistemática en contra de periodistas y defensores de derechos humanos en México”, realizado por Artículo 19, R3D y Social Tic, con asistencia de Citi Lab de la Universidad de Toronto, Canadá, expone las prácticas de ciberespionaje efectuadas por el Estado mexicano a través de la instalación del “malware Pegasus”, el cual accede a todos los contenidos y funciones de los celulares infectados como: activar cámaras y micrófonos, acceso a mensajes, fotos, contactos, agendas y aplicaciones que transfieren la información en tiempo real mediante Internet: las soluciones han sido poco consecuentes con el contexto de nuestra realidad.

El espionaje electrónico (ciberespionaje), se desarrolla con celeridad y son muy pocos los sistemas de seguridad que puedan ser inquebrantables ante esta clase de transgresiones. Asimismo, son una minoría los países que cuentan con una legislación sobre esta actividad, situación que, desde luego, dificulta, en gran, medida su identificación y las posibilidades de una adecuada sanción.

Pero más allá del hecho de castigar a los responsables ─que no es una cuestión menor─ se encuentra el problema de fondo respecto al espionaje cibernético, como son: las acciones que ponen en riesgo y atentan contra la seguridad nacional y la soberanía de México, al infiltrar las comunicaciones institucionales y la amenaza que representa para los individuos al violar su derecho a la privacidad.

De esas líneas surgen las siguientes preguntas de investigación: ¿Qué es el espionaje electrónico o ciberespionaje? ¿Es un comportamiento antisocial aislado o es un delito generalizado? ¿Es más importante la seguridad nacional que el derecho a la privacidad de un individuo? ¿El término seguridad nacional en México corresponde a las actuales condiciones políticas, económicas y sociales que se viven a nivel nacional e internacional? ¿Qué se entiende en México por amenaza a la seguridad nacional? ¿La definición del delito de espionaje en México es consecuente con la realidad en la que vivimos?

Con base en lo anterior, la hipótesis de este trabajo de investigación es: las instituciones garantes de la seguridad nacional en México se han caracterizado por la práctica generalizada para recopilar información (espionaje), una consecuencia de su estrecha relación con el sistema político. Por otro lado, la normatividad mexicana descuida el impacto que tienen las nuevas tecnologías al modificar el concepto de espacio o ámbito en el que se manifiestan, profundizan y desarrollan los derechos humanos. Es decir, omite una adecuada reformulación de los derechos de primera, segunda y tercera generación en el entorno del ciberespacio, un obstáculo para el surgimiento de la cuarta generación de derechos humanos. Como resultado, la regulación del delito de espionaje en

México tiene un enfoque acotado por carecer de una adecuada reflexión sobre el impacto de las ciberamenzas, en particular, el ciberespionaje.

Aunado a lo anterior se suman: si no existe una adecuada delimitación del delito de espionaje electrónico entonces las amenazas se potencializan mediante el abuso en el uso de las Tecnologías de la Información y Comunicación. Igualmente, si persiste el conflicto político jurídico entre el derecho a la privacidad y la seguridad nacional entonces las actuales políticas públicas no garantizarán los derechos humanos en el ciberespacio. Además, la persistente ambigüedad para definir que es una amenaza para la seguridad nacional en México y la acotada definición de espionaje genera que el marco jurídico de la intervención de comunicaciones en México no sea consecuente con la realidad.

Durante la exposición de los tres capítulos que comprenden esta tesis, se busca que el Estado Mexicano tome conciencia sobre la amenaza que representa el ciberespionaje y la regule por medio de la creación de un cuerpo institucional.

La relevancia de las instituciones se encuentra en que conforman la base de cualquier sistema político, porque reducen la incertidumbre al proporcionar una estructura a la vida diaria, es decir, son una guía para la interacción humana.

El nuevo institucionalismo o neo institucionalismo, en su búsqueda de acciones más consecuentes con la realidad, emplea un enfoque y una metodología interdisciplinaria que nos permitirá comprender la relación de las instituciones con el Estado, comparando el pasado y el presente de las mismas para entender la relación entre la decisión individual y la político-social del futuro. Esta corriente se caracteriza entonces porque vuelve a situar al Estado como núcleo de la política mundial, aunque reconoce la existencia de otros actores subordinados a éste, se pronuncia por la cooperación estatal y de instituciones internacionales a fin de superar la anarquía en el sistema global, observa los principios de reciprocidad y respeto de las normas; y, por incremento de los procesos de integración regional y en todo el mundo.

En el primer capítulo se definen los términos neo institucionalismo, seguridad nacional, soberanía y espionaje electrónico desde la óptica de las Relaciones Internacionales.

Un enfoque plural que sin duda nos ayudará a comprender el reto que representa el espionaje electrónico para las instituciones, en especial aquellas garantes de los derechos humanos. Del mismo modo, nos permita observar que día a día la información es robada tanto de las redes del sector privado como del gobierno; penada según el orden interno y la costumbre en casi todas las naciones del mundo; que roba secretos comerciales, estrategias de mercado e información confidencial de empresas, gobiernos e individuos; que causa pérdidas económicas a gran escala; que realizan individuos que operan al amparo de las lagunas jurídicas existentes; y, con un impacto internacional de la cual desconocemos cuáles serán las consecuencias.

En el segundo capítulo se analizan las políticas públicas en materia de espionaje electrónico, realizadas por las naciones con mayor conocimiento del tema (Estados Unidos de América, Federación Rusa, República Francesa, República Federativa de Brasil, República Federal de Alemania y República de Estonia).

Se exponen los casos más emblemáticos, en donde las consecuencias negativas para los individuos han sido incontrovertibles. Mientras que el Estado ha amparado sus acciones en la visión tradicional de seguridad nacional; en donde el Estado sigue siendo el actor principal y el uso de la fuerza el instrumento fundamental.

Desde la perspectiva del Sistema Universal de Protección de los Derechos Humanos de Naciones Unidas, dos objetivos son importantes en materia de protección de la privacidad de los individuos. El primero es la Declaración Universal de los Derechos Humanos y, el segundo, el Pacto Internacional de Derechos Civiles y Políticos. En ambos casos se establece que nadie debe ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o

correspondencia y, además, que toda persona tiene derecho a la protección de la ley contra esas injerencias.

En el tercer capítulo, se recapitulan los antecedentes de las instituciones que salvaguardan la soberanía nacional en México. Se constata cuáles son los órganos responsables de la seguridad nacional mexicana y se analiza la actuación de las instituciones responsables de la seguridad nacional, en los casos de espionaje electrónico, realizados por el gobierno mexicano a periodistas y defensores de derechos humanos en México, mediante el marco jurídico mexicano en materia de seguridad nacional en que se sustenta la intervención de comunicaciones privadas.

Por último, se busca contribuir con una propuesta de políticas públicas para regular el espionaje digital, en donde se garantice la rendición de cuentas para la existencia de una Internet libre. En donde la privacidad y la seguridad puedan coexistir en un contexto de Derechos Humanos. Un marco jurídico nacional que regule legítimamente esta actividad desprendida del ejercicio constitucional de la defensa de la soberanía y la garantía de las libertades públicas y privadas. Además de un marco institucional que vele por el cumplimiento de estas normas.

Se busca, en última instancia, conocer las dificultades que enfrentan las naciones para desarrollar marcos jurídicos que regulen el ciberespionaje, en casos concretos: el anonimato en internet, el desarrollo exponencial de la tecnología, la reducción de costos y tiempo, la correcta aplicación de medidas de seguridad y la ingeniería social. Para ello, tal vez sea el momento de dejar de ver a la privacidad como un costo de la seguridad y empezar a verla como un beneficio. Puesto que, la privacidad es seguridad y deben de ir acompañadas.

CAPÍTULO 1 MARCO TEÓRICO-CONCEPTUAL

El progreso del ser humano plantea el uso de todos los recursos disponibles y la creación de diversas tecnologías, para facilitar su bienestar. Estas transformaciones nos conducen día a día a nuevas situaciones y planteamientos. Sin embargo, todas deberían llevarnos a un estudio consiente y profundo de sus efectos para tomar decisiones que marquen el camino hacia la sociedad que deseamos construir.

En una era, en donde el uso de las Tecnologías de la Información y Comunicación (TIC) es un elemento fundamental en nuestra sociedad, debido a que no existe persona, organización, empresa o gobierno alguno que ignore los avances en sistemas computaciones y comunicacionales, se requiere de modificaciones en la política pública a escala nacional y mundial para controlar las transformaciones tecnológicas actuales que, si bien es cierto, han generado nuevas oportunidades, vínculos, negocios y hasta relaciones personales, también han facilitado la realización de actividades negativas como la existencia de conductas antisociales y de nuevos delitos.

Es ante este escenario que resulta imprescindible una sociedad con capacidades que faciliten las transformaciones y el fortalecimiento en importantes áreas de la humanidad y no solo una sociedad revolucionada entorno a la información, se busca una sociedad consiente con capacidad de decisión que facilite el aprendizaje de sus individuos para construir una sociedad en donde prevalezca el conocimiento.

Este capítulo, tiene como propósito la comprensión conceptual de los términos neo institucionalismo, seguridad nacional, soberanía y espionaje electrónico desde la óptica de las Relaciones Internacionales. Un enfoque plural que sin duda nos ayudara a comprender el reto que representa el espionaje electrónico para las instituciones en especial aquellas garantes de los derechos humanos. Del mismo modo, nos permita observar que día a día la información es robada tanto de las redes del sector privado como del gobierno, una actividad penada según el orden interno y la costumbre en casi todas las naciones del

mundo, una actividad que roba secretos comerciales, estrategias de mercado e información confidencial de empresas, gobiernos e individuos, una actividad que causa pérdidas económicas a gran escala, una actividad que realizan individuos que operan al amparo de las lagunas jurídicas existentes, una actividad de impacto internacional de la cual desconocemos cuáles serán las consecuencias futuras.

Para dar sustento a estas afirmaciones se expondrán los fundamentos de los principales teóricos de los conceptos empleados; además se analizará el uso de los mismos con el objetivo de identificar su significado en la normatividad mexicana y la aplicación en el sistema internacional.

1.1 Neoinstitucionalismo

Conocer la arquitectura de nuestra sociedad es vital para la adecuada convivencia entre los seres humanos. Es indispensable entender que nuestra realidad está basada en mitos, dogmas, ideologías y verdades particulares. Es necesaria la comprensión de las aspiraciones así como las decisiones de los individuos, porque es a nivel individual que el conocimiento tiene una característica esencial. La explicación es sencilla, las personas toman decisiones con base en el conocimiento que poseen, conocimiento que nos permite afrontar los diversos problemas sociales, políticos, culturales, económicos, etc.

Así mismo, los Estados son entidades dinámicas, los cuales deben adaptarse y transformarse para mantener una vigencia idónea con el entorno internacional, este componente implica la búsqueda y la consolidación de nuevos intereses estratégicos, que fortalezcan a la nación para asegurar su permanencia en la comunidad internacional.

Es así que los términos de seguridad nacional, soberanía y orden institucional son principios determinantes en el proceso de continuidad del Estado Mexicano, porque construyen y orientan el conocimiento hacia mecanismos de desarrollo a largo plazo. Del mismo modo vinculan el cambio en la conducta

humana a través del tiempo al señalar la evolución, el cumplimiento, las limitaciones y las posibles afectaciones por el mal funcionamiento de los mismos.

Sin embargo, al tratarlos como algo exógeno al sistema o como factores constantes, se deja de lado el estudio de su incidencia en el sistema. Es necesario recordar que son los procesos y los fenómenos sociales y políticos el primer contacto que tienen nuestros sentidos con el entorno. Aquellos que no son evidentes en sí mismos, pero si son determinantes en nuestra experiencia porque requieren de un análisis que sintetice y sistematice los métodos para su correcta aplicación.

La actual interdependencia que tiene nuestro país con la comunidad internacional es un ejemplo de lo anterior. Aunque se puede explicar mediante múltiples factores, quizá el más importante es el fenómeno de la globalización que incorpora una serie de transformaciones sociales. Desde la liberalización y democratización de los ordenamientos político, jurídico y económico hasta la actual revolución de las Tecnologías de la Información y Comunicación.

Son estas experiencias distantes que afectan en mayor o menor medida a los Estados y sus paradigmas. Los atentados del 11 de septiembre de 2001 son ejemplo de ello, los cuales afectaron al mundo y a las definiciones que existían entorno a conceptos como seguridad nacional y soberanía; así mismo, provocaron el surgimiento de nuevos términos como: el terrorismo, las leyes preventivas y los ciberdelitos.

Es desde una perspectiva objetiva e integral ante la era de las Tecnologías de la Información y Comunicación que debemos analizar el tema del espionaje electrónico en México. Es necesario considerar los riegos y las amenazas que representa, debe ser una preocupación que mueva a sus instituciones y a la sociedad en general a mantener una actitud responsable entorno a él.

En los años recientes, el Estado Mexicano fue víctima del “Grupo Equation”[1] responsables del espionaje electrónico global que atacó la infraestructura informática de más de treinta países con el apoyo de la Agencia de Seguridad Nacional estadounidense.

En México se detectó un nivel "medio de infección"[2] de estas herramientas, principalmente en los sectores de gobierno y financiero, aunque se desconoce el impacto de esta campaña de ataques cibernéticos en contra de la infraestructura de gobierno. Sin embargo, las soluciones han sido poco consecuentes con el contexto de nuestra realidad.

Como ya se ha mencionado en párrafos anteriores, las instituciones tienen efecto en las acciones de los individuos y como es lógico en una nación, porque sirven para generar un ambiente de participación y coordinación. Al trascender voluntades individuales, al identificarse con un propósito, buscan los componentes ideales de una entidad para satisfacer necesidades sociales y éticas, creadoras de reglamentos, códigos, o inclusive constituciones. Es decir, que los cambios hechos en las instituciones tendrán consecuencias en el comportamiento de los Estados y por ende, de los individuos.

Por lo tanto, el nuevo institucionalismo o neo institucionalismo estudia la relación de las instituciones con el Estado, comparando el pasado y el presente de las mismas para entender la relación entre la decisión individual y la político-social del futuro.

Su propósito es explicar el desarrollo de las naciones, mediante un mayor grado de autonomía en el funcionamiento de las instituciones porque son fundamentales para determinar el cambio, la estabilidad e incluso la inestabilidad de un determinado sistema político y de la propia política respetivamente, sin apartarse de la norma jurídica. Del mismo modo aprecia la importancia de las

---

[1] Kasperskylab “Grupo Equation: El creador principal del ciberespionaje”, [en línea], 22 de abril de 2016, en http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/2015/grupo-equation-el-creador-principal-del-ciber

[2] “Introducción a la seguridad en Internet y aplicaciones”, [en línea], 22 de abril de 2016, en http://www.capacinet.gob.mx/Cursos/Tecnologia%20amiga/desarrolladordesoftware/Seguridad_Internet_SE.pdf

tareas ejecutadas por los individuos y el Estado. Sin embargo, será el entorno de vital importancia para explicar la influencia social, económica, política y cultural sobre nuestras conductas.

El neo institucionalismo surge en las décadas de 1970 y 1980 en respuesta a la vertiente internacional y, al mismo tiempo, como crítica a la rigidez analítica de la economía neoclásica, en donde la premisa fundamental era el control de los individuos a través de las instituciones. Entre sus autores se encuentran: James Gardner March, Johan Peder Olsen, Paul DiMaggio, Walter Woody. Powell, Oliver Williamson, Philippe C. Schmitter, Stephen Krasner, Meyer y Scott.

Aunque el principal exponente de la teoría neo institucionalista es Douglas North al mencionar que: "el Estado es una organización de la sociedad con ventaja competitiva en la violencia y que ofrece servicios, entre ellos el de fijar los derechos de propiedad y fijar las reglas de intercambio social, al tiempo que brinda protección y seguridad. El Estado media las relaciones entre los grupos sociales, obliga al cumplimiento de los contratos, impone las normas de comportamiento social y beneficia a unos grupos en detrimento de otros. Esa organización es la encargada de imponer las reglas del juego social, de impartir justicia y de castigar a los infractores.

Así, el Estado pone muchas de las reglas sociales y a su vez se rige por las reglas en su funcionamiento interno y en la relación con sus competidores. Estas reglas se convierten, al paso de la historia, en las leyes de diverso orden; la forma moderna de expresar y clarificar las reglas del juego en las sociedades".[3]

El neo institucionalismo en su búsqueda de acciones más consecuentes con la realidad emplea un enfoque y una metodología interdisciplinaria que integra la economía; con modelos más dinámicos, el derecho; con la teoría de los contratos, la sociología; con la teoría de las organizaciones al generar un mayor grado de afinidad con base en las tradiciones, los hábitos, los valores y los roles de los individuos, la psicología; con su análisis de la conducta humana y la historia; con su intento de explicar el rol que han tenido todos ellos.

[3] Romero Jorge Javier, "Para entender las Instituciones Políticas", p. 7.

Sin embargo, al ser una visión polifacética el neo institucionalismo tiene diferentes enfoques como el neo institucionalismo económico, el neo institucionalismo político, el neo institucionalismo sociológico, el neo institucionalismo histórico.

"Los citados neo institucionalismos suelen agruparse en tres grandes familias (Hall y Taylor, 1996): en primer lugar, el conjunto de trabajos englobados en el marco del neoinstitucionalismo económico y las teorías de la elección racional, que se alinean (aunque modificándola) con la idea de racionalidad económica; en segundo lugar, los estudios enmarcados en el institucionalismo histórico, heredero de los análisis de los así llamados "macroanalíticos" de la política comparada como Moore (1973) o Skocpol (1984); y por último, el denominado "institucionalismo sociológico"-o sociología económica-."[4] Aunque todos ellos comparten una idea central: la importancia de las instituciones.

El concepto de institución es extremadamente amplio y complejo porque en nuestro lenguaje cotidiano, el término institución se aplica a entidades totalmente diferentes como: la iglesia, el matrimonio, la familia, el nuevo reglamento de tránsito, la Ley del Servicio Exterior Mexicano, etc. A todo esto, llamamos institución, sin embargo, persiste la pregunta ¿Qué es una institución?

Douglas North señala que "…las instituciones son las reglas del juego en una sociedad, o más formalmente, son las limitaciones ideadas por el hombre que dan forma a la interacción humana y estructuran incentivos en el intercambio humano": reducen la incertidumbre, simplificando la vida.

En palabras de March y Olsen: "…son el conjunto de reglas y rutinas interrelacionadas que definen las acciones apropiadas en términos de las relaciones entre roles y situaciones".[5]

"En casi todos sus usos el concepto de institución connota la presencia de reglas compartidas que son vistas como vinculantes por los actores sociales, y

[4] H. Acuña Carlos, "¿Cuánto importan las instituciones? Gobierno, Estado y Actores en la política argentina", p. 23.
[5] Nuevo institucionalismo y políticas públicas, [en línea], 20 de mayo de 2016, en http://www.aecpa.es/uploads/files/congresos/congreso_09/grupos-trabajo/area06/GT01/08.pdf

que estructuran sus actividades y sus interacciones recíprocas, al igual que las reglas que regulan la práctica de un deporte estructuran las actividades y las posibles interacciones de los jugadores que lo practican."[6]

Las instituciones, en un sentido amplio, son padrones compartidos de expectativas, las reglas del juego, colecciones de costumbres y rutinas, organizaciones formales y procedimientos informales, leyes, normas, códigos y paradigmas de restricciones sociales, sistemas de incentivos compartidos, rutinas cuasi naturales, equilibrios de comportamiento, son las redes que sirven para enlazar y encauzar institucionalmente las relaciones de intercambio económico, social y político.

Las instituciones han adquirido a lo largo de la historia diversas formas, aunque se les puede dividir en dos grandes grupos: aquellas que requieren del Estado para operar y aquellas que se reproducen autónomamente como una manera de hacer las cosas de una comunidad concreta —todo eso que llamamos cultura— y que incluyen los valores morales, tradicionales, las prácticas religiosas colectivas, la sanción social en el trato o la manera de entender la convivencia y la ley. Por supuesto que los grupos se refuerzan mutuamente: el Estado, para imponer las reglas formales tiene que contar con la aceptación mayoritaria de sus actos, y a la vez, históricamente, los valores morales de origen religioso fueron inculcados con ayuda de la coacción física y la violencia del Estado.[7]

La relevancia de las instituciones se encuentra en que conforman la base de cualquier sistema político porque reducen la incertidumbre al proporcionar una estructura a la vida diaria, es decir, son una guía para la interacción humana. A través de ellas se estructuran los procesos de socialización, participación e interacción social y política.

Entre las principales características de las instituciones están: **el origen social**, porque no son ni hechos naturales ni productos divinos, **la extensión social,** prácticas y conocimientos compartidos, **la extensión temporal** son

[6] Del Castillo Arturo, "El Nuevo Institucionalismo en el análisis organizacional: Conceptos y enunciados explicativos", p. 3.
[7] Romero Jorge Javier, *Op. Cit.*, p. 7.

estables, perdurables, permanentes y persisten en el tiempo, **la función social**[8] establece restricciones y abre oportunidades en el comportamiento, la interacción, las expectativas o las percepciones.

Cabe señalar que dentro del neoinstitucionalismo una cuestión que ha demandado atención está referida al "cambio institucional" partiendo de que este último delinea la forma en que la sociedad evoluciona en el tiempo y es, a la vez, la clave para entender el cambio histórico. Además, dentro del proceso de cambio institucional, según Paul DiMaggio, tendríamos o incluiríamos a cuatro momentos o etapas de saber:

a) La formación institucional.

b) El desarrollo institucional.

c) La desinstitucionalización.

d) La reinstitucionalización.[9]

El neo institucionalismo en primer lugar, trata de explicar el comportamiento del Estado a través de la compresión de la naturaleza del sistema internacional; es decir, el neoinstitucionalismo reconoce que las instituciones funcionan en un entorno compuesto por otras instituciones, llamado el entorno institucional. Cada institución se ve influida por un entorno más amplio. En este entorno, el principal objetivo de las organizaciones es sobrevivir. Con el fin de hacerlo, tienen que hacer algo más que tener éxito económicamente, necesitan establecer su legitimidad dentro del mundo de las instituciones.

En palabras de la investigadora Claudia G. Jiménez González, en el neoinstitucionalismo, el objeto central es el Estado "como estructura política de

---

[8] "Neoinstitucionalismo", [en línea], 22 de mayo 2016, en https://books.google.com.mx/books?id=QK79r_mPPG8C&pg=PA472&lpg=PA472&dq=Las+instituciones+sociales+son+creaciones+sociales;+no+son+ni+hechos+naturales+ni+productos+divinos:+el+origen+social+de+las+instituciones.&source=bl&ots=LI7wrhOC7N&sig=btX5FIUfdHX3wMRkx1TQSiPoyWM&hl=es-419&sa=X&ved=0ahUKEwiBp66kLMAhUh2oMKHeK1AUQQ6AEIGjAA#v=onepage&q=Las%20instituciones%20sociales%20son%20creaciones%20sociales%3B%20no%20son%20ni%20hechos%20naturales%20ni%20productos%20divinos%3A%20el%20origen%20social%20de%20las%20instituciones.&f=false

[9] "El neoisntitucionalismo y la revalorización de las instituciones", [en línea], 22 de marzo de 2017, en http://www.redalyc.org/pdf/110/11000903.pdf

tipo formal que representa el poder político", en tanto entidad de dominio institucionalizado que ofrece respuestas a nivel de organizaciones participantes de la vida política y social de las naciones, sean estas partidos políticos, legislaturas, iglesias o cualquier otra forma que tenga representatividad, cuyas propuestas son de tipo normativo y sistemáticas en torno de los actores mencionados.

En esta teoría el neoinstitucionalismo formaría parte del marco que daría estabilidad al estado a cambio de que haya obediencia de las normas impuestas, de lo contrario las consecuencias serían la aplicación estricta del marco regulatorio del Estado que es la indudable aplicación de la Ley sin distinciones, por lo tanto del comportamiento social se deduce que las preferencias de los ciudadanos serían satisfechas por las instituciones.

En segundo lugar, reafirma la idea de que las instituciones y las estructuras pueden cambiar como consecuencia de la acción humana y, por lo tanto, los procesos generados ejercen profundos efectos en el comportamiento del Estado; menciona que el comportamiento humano es influenciado por las instituciones a través de reglas, normas y otros marcos. Y esta influencia actúa de dos principales formas: puede hacer que los individuos maximicen los beneficios dentro de las instituciones o puede hacer que los individuos actúen fuera de servicio, abandonando la conciencia de lo que se supone es su deber porque no pueden concebir ninguna alternativa.

En tercer lugar, introduce el papel de la cultura como elemento importante en la formación de identidades individuales y sociales plantea que la cultura es una construcción que, a su vez, es un producto de la interdependencia entre individuos y grupos. Es decir, las creencias culturales y las reglas que estructuran el conocimiento son la guía en la toma de decisiones a nivel de organizacional porque centran la atención de los tomadores de decisiones en un conjunto delimitado de los problemas y soluciones que conduce a decisiones lógicas consistentes que refuerzan las identidades existentes de organización y sus estrategias.

"Esta corriente se caracteriza entonces porque vuelve a situar al Estado como núcleo de la política mundial, aunque reconoce la existencia de otros actores subordinados a este, se pronuncia por la cooperación estatal y de instituciones internacionales a fin de superar la anarquía en el sistema global, observa los principios de reciprocidad y respecto de las normas; y, por incremento de los procesos de integración regional y en todo el mundo".[10]

1.2 Antecedentes y concepto de soberanía

El resurgir del interés por estudiar las instituciones obedece y es la consecuencia de los diversos cambios y transformaciones experimentados en el seno de la sociedad, en el funcionamiento del Estado (cada vez más complejo y diferenciado). Además, la mayoría de los principales agentes en los sistemas políticos y económicos modernos son organizaciones formales, procedimientos, instituciones legales, prácticas institucionalizadas y demás que, ciertamente, tienen un papel dominante en la vida contemporánea y en la propia constitución de la sociedad. Las instituciones articulan y desarticulan, estructuran y desestructuran, integran y desintegran, promueven y restringen nuestras conductas, nuestras reglas, códigos, tradiciones, etc.

Y es justo en ese sentido cuando nos preguntamos: ¿Cuál es papel del Estado, la soberanía y la seguridad nacional? ¿Cuál es la jurisdicción de las instituciones? ¿Hasta dónde llegan los derechos de los Estados y donde empiezan los de la comunidad internacional en un sentido genérico? ¿Dónde quedan los valores compartidos por la comunidad internacional como la democracia, los derechos humanos, el libre mercado y la conservación del planeta?

[10] Jiménez González, Claudia G., "Las teorías de la cooperación internacional dentro de las relaciones internacionales" [en línea], 29 de marzo de 2016, en http://www.juridicas.unam.mx/publica/librev/rev/polis/cont/20032/art/art5.pdf

Teóricos realistas como *Morgenthau* han sugerido que: “No importa, cuáles son los fines últimos de la política internacional el poder siempre será el objetivo inmediato”.[11]

Sin embargo, la edificación de un sistema de valores con el que armonicen todos los pueblos y la existencia de unas instituciones que los respalden, a fin de evitar el conflicto de intereses, es una aspiración que comparten las corrientes de pensamiento más influyentes de los últimos dos siglos.

La superación de los intereses inmediatistas y “mezquinos” de los Estados es señalada con frecuencia como la solución para arribar a una situación superior, en la que la humanidad, sin distingos ni divisiones, comparta un universo de valores comunes.

No obstante, ¿cuál es el origen de Estado? ¿Cuáles fueron las opiniones que influyeron en la formación de las instituciones políticas existentes? Para conocer los hechos que dieron origen al Estado se ha retomado la obra de Francisco Porrúa Pérez, “Teoría del Estado”[12], en la cual menciona algunos hechos importantes:

Durante los siglos XVII, XVIII y XIX, el Estado Constitucional tuvo su origen con John Locke, Charles Louis de Secondat (Montesquieu), Jean-Jacques Rousseau, Thomas Jefferson y el abate Emmanuel-Joseph Sieyès, pensadores liberales que sostenían: se debía poseer una constitución no otorgada, introducir la división de poderes y garantizar los derechos fundamentales.

Aunque es a Nicolás Maquiavelo a quien se atribuyó la introducción del “Estado Moderno” con su obra “El Príncipe”, estableciendo: “Los Estados y soberanías que han tenido y tienen autoridad sobre los hombres fueron, y son, o repúblicas o principados”[13]. Lo considera como uno de los ingredientes

---

[11] “Estado, soberanía y seguridad nacional”, [en línea], 17 de mayo de 2017, en http://www.cisan.unam.mx/pdf/lc02_03.pdf

[12] “Capítulo II: El Estado y su origen”, [en línea], 20 de mayo de 2017, en http://catarina.udlap.mx/u_dl_a/tales/documentos/ledf/priego_s_g/capitulo2.pdf

[13] Ibídem, 26.

fundamentales de la comunidad política, y que, al convertirse en soberanía, dio origen al Estado moderno.

El estado, la máxima organización política, es un hecho social, un fenómeno resultado de la convivencia humana y únicamente realizable a través del dominio de la cultura que comprende cada acto del hombre en busca de un fin llamado perfección.

No obstante, por ser una construcción humana, el Estado tiene fines colectivos, de todos los miembros de su sociedad, y ¿cuáles son?:

a) "Crear un orden necesario;
b) Asegurar la convivencia social;
c) Establecimientos de medios para el desarrollo cultural, económico, político, moral y social;
d) El bienestar de la nación; y
e) La solidaridad social."[14]

Para ser el Estado la máxima organización ha empleado el derecho y la autoridad que al conjuntarse crean una intrincada red institucional, parte de ella son los elementos que conforman el Estado:

1. Población: Es el conjunto de hombres y mujeres (habitantes) que forman parte de una comunidad, asentada en un territorio (un área geográfica determinada o determinable) que persiguen un fin político e ideológico.
2. Territorio: Es la porción de tierra, agua y espacio donde opera el Estado.
3. Gobierno: Autoridades que dirigen, controlan y administran las instituciones (el conjunto de organismos que institucionalizan al poder y que cohesionan a la sociedad a través del gobierno) del Estado.
4. Soberanía: Cualidad del poder del Estado que le permite autodeterminarse y autogobernarse libremente sin la intervención de otro poder de tal manera que el Estado soberano dicta su Constitución y señala el contenido de su derecho.

[14] "Teoría del Estado", [en línea], 17 de mayo de 2017, en https://archivos.juridicas.unam.mx/www/bjv/libros/3/ 1461/5.pdf

La soberanía, elemento esencial de los Estados modernos. Considerada al interior del Estado como el ejercicio del poder supremo, al exterior de él como la independencia en la medida que el poder se ejerce en condiciones de igualdad y respeto frente a otro poder.

Denominada como una potestad suprema e independiente para determinar el contenido concreto del orden Jurídico, una capacidad jurídica y real de decidir, la facultad absoluta de autodeterminarse mediante la expedición de una Ley Suprema que tiene una Nación.

Sin embargo, la concepción de soberanía en la historia es confusa debido a que este concepto tiene definiciones poco concretas. El problema reside en la semántica de los términos y expresiones de una época o civilización porque al ser traducidos de un idioma, época o civilización a otro, este solo puede darle equivalentes aproximados. Otra propensión que agrava esta problemática es "nuestra tendencia a suponer que en los términos antiguos aún en uso actualmente el fenómeno real que una vez hubo debajo o detrás de ellos no ha experimentado cambio alguno".[15]

"El término soberanía originariamente y durante mucho tiempo expresó la idea de que hay una autoridad final y absoluta en la comunidad política".[16] El concepto se formuló cuando las circunstancias produjeron rápidos cambios, cuando se combatió la estrecha integración entre sociedad y gobierno. Es decir, el origen y la historia del concepto de soberanía se hallan estrechamente vinculados con la naturaleza, origen e historia del Estado; pero no surgirá hasta que el debido proceso de integración o de conciliación haya tenido efecto entre un Estado y su comunidad.

La soberanía es el concepto con el que el hombre ha tratado de apoyar las viejas ideas de legitimación y de responsabilidad o con el que ha contado para fundamentar las nuevas versiones de estos medios por los que el poder se convierte en autoridad. Su función en la historia de la política ha sido la de reforzar

[15] Hinley F.H., "El concepto de soberanía", p. 27.
[16] ibídem, p. 9.

las reivindicaciones del poder o bien los procedimientos por los que el poder político puede ser llamado a rendir cuentas, una nueva solución de un problema existente, un nuevo estilo de pensamiento sobre el poder y el gobierno.

"El concepto de soberanía es solo un replanteamiento del problema permanente de determinar la base del gobierno y la obligación dentro de una comunidad política, por otra parte, no es más, que el replanteamiento del problema que se crea cuando la comunidad política y su gobierno se juzgan recíprocamente necesarios y autosuficientes y que se mantendrá todo el tiempo que se juzguen de este modo".[17]

La base de la concepción tradicional de la soberanía la encontramos principalmente en los doctrinarios de la época moderna, principalmente en los humanistas de los siglos XVI y XVII, y a partir de entonces se ha considerado invariablemente como el principio que constituye uno de los caracteres esenciales del Estado. Es por eso, que el estudio de la problemática actual del principio de soberanía en el Estado Nacional, difícilmente puede llevarse a cabo prescindiendo de las aportaciones de los doctrinarios de la etapa moderna, pues tal omisión vaciaría de sentido el análisis de una institución que es configurada teóricamente por los doctrinarios de esa época, pues si bien se han dado muestras de evolución en el transcurso del tiempo, resulta del todo imprescindible tener como referencia o punto de partida la edificación doctrinal de ese principio.

El principio de soberanía se consolida en los inicios de la edad moderna, aunque cuenta con algunos precedentes desde la antigüedad, en la que se establecieron concepciones en torno a la comunidad política y a las formas de organizar el poder. Así, los griegos identificaban al gobernante con la ley; en tanto que: "la noción del imperio del pueblo romano (*imperium populi Romani*; representaba la máxima extensión de la idea de la polis) era el poder para gobernar que el pueblo romano confería a sus más altos representantes y este poder y este título podían poseerlo varios individuos simultáneamente. Dado que eran otorgados por el pueblo, podría suponerse que este era concebido como

[17] Ibídem, p. 29.

pueblo soberano".[18] Estas concepciones estaban alentadas por un ideal de satisfacción de la unidad social, más que por un ideal configurador del poder soberano. Posteriormente, Roma transmitió la concepción de soberanía a la edad media, se justificó la legitimación del poder por orden divino, con un pensamiento teocrático que fue cediendo paso paulatinamente a la concepción normativa o del derecho en la organización política, surgiendo con ello, una diferenciación entre ley divina y ley emanada del poder político, dejando de concebirse a este solo desde el orden de lo moral y lo divino.

Las doctrinas sobre la soberanía a principios de la época moderna surgen como una respuesta al conflicto y a la crisis generada a finales de la Edad Media, en la concentración del poder no se encontraba claramente definida en un titular sino disperso en varias instituciones: en el rey, la iglesia, la aristocracia y el pueblo; o por la crisis de las constituciones mixtas en la que el poder estaba repartido entre varios factores, teniendo como origen la concepción moderna de la soberanía la necesidad de justificar el poder supremo en una de las diversas instituciones de la comunidad política.

En la fase más reciente de la historia la instauración definitiva de la soberanía como concepto predominante en el campo de las definiciones políticas vigentes ha sido un reflejo de la constante integración de la comunidad política y del poder del Estado.

Finalmente, la adecuada comprensión de la naturaleza y de la función de este concepto puede mostrarnos que "ni en su historia ni como ciencia política puede propiamente usarse para explicar –o justificar siquiera– lo que el Estado o la sociedad política haga o pueda hacer. Se trata de un principio que sostiene solamente que debe existir una autoridad suprema dentro de la comunidad política, para que la comunidad pueda existir, o cuando menos para que pueda actuar tal como exigen su carácter y las circunstancias. Nada más fácil que pasar de esta interpretación adecuada del principio a su uso inadecuado o excesivo que tan a menudo ha prevalecido en los últimos tiempos. La evidencia de la

[18] Ibídem, p. 39.

historia muestra, en efecto, que la democracia moderna o el Estado constitucional no han sido más reacios a practicar esta distorsión que las regencias personales cuando trataron de uncir el concepto al carro de algún emperador absoluto en los tiempos de Roma o al derecho divino cuando la moderna reaparición del concepto. Pero lo cierto es que si se hace esta transición no se comprende la función de la soberanía; como lo es que el hecho de errar en la comprensión del concepto por parte de los que dudaron de su validez y aceptar su uso por parte de los que han extorsionado su sentido en interés del poder ha sido un segundo factor que ha fomentado en gran manera la reprobación moral".[19]

Algunos teóricos como: Aristóteles, Grocio, Bodino, Del Vecchio mencionan que es: una autoridad creada por el pueblo y que al mismo tiempo acepta delegar el poder en sus representantes. Otorgándoles el derecho de tomar decisiones con independencia de poderes externos: siendo así la máxima autoridad dentro de un sistema político.

En el área de las Relaciones Internacionales, la soberanía se ostenta como la independencia que debe tener un Estado, tanto de acción como de decisión frente a otros Estados con voluntad soberana para concretar el ejercicio de sus poderes. El Estado es autónomo para darse a sí mismo su estructura, su organización y decidir en todo aquello que concierne a su gobierno y los problemas que le afecten en su aspecto interno. Entendida así la problemática, puede afirmarse que cualquier intervención que sufra el Estado, sobre diversas cuestiones por parte de otra organización política, debe ser considerada como una agresión a la soberanía, que puede tener severas consecuencias como un posible conflicto bélico.

La doctrina sostiene que, ante la existencia de Estados soberanos, el derecho Internacional se encuentra equilibrado porque sus miembros son soberanos e iguales; cada uno dentro de su propio ámbito territorial es una unidad decisoria autodeterminada, que en el ámbito externo debe tener los mismos derechos y obligaciones. La actual posición internacional en lo referente al tema

[19] Ibídem, p. 187.

de la soberanía no hace justicia a la realidad política, por no estar acorde con ella. Los Estados, los organismos no gubernamentales, las empresas transnacionales, las instituciones tienen una interdependencia económica, política y cultural entre sí y una catástrofe en cualquiera de estas áreas de cualquier Estado, puede generar nefastas consecuencias en otro.

Las siguientes son algunas definiciones en el acervo del concepto de soberanía; donde podemos identificar una diversidad de apreciaciones:

La sociedad griega un referente en los campos de estudio relativos al Estado, la sociedad y el Derecho, reconocieron que la capacidad de ser autónomos y autosuficientes concedía una independencia digna de ser defendida. Aristóteles uno de sus más grandes filósofos indica que la soberanía es “la organización política, el Estado-Ciudad es la vida buena de los iguales”, es decir la independencia del Estado y el respeto del exterior se basa en su capacidad para satisfacer todas sus necesidades más que su naturaleza de poder supremo.

En el siglo XVI encontramos al filósofo-político francés Juan Bodino quien define la soberanía como “el poder supremo sobre los ciudadanos y súbditos, no sometidos a las leyes”. Bodino consideraba que el Estado es un gobierno de varias familias que al unirse en asociaciones y conformar comunidades creaba lo que denomino el Estado soberano, sobre esta unión reinaba de manera incondicional e ilimitada quien recibía el derecho de gobernar. Los reyes o soberanos detentaban de manera ilimitada el poder, con la única excepción de ser responsables ante Dios y el Derecho Natural.

Para el humanista holandés Hugo van Groot o Hugo Grocio en su obra, Del derecho de la guerra y la paz, demuestra su consonancia con el derecho internacional. Por lo que sus escritos tuvieron la finalidad de establecer una base para las relaciones jurídicas entre los estados autónomos, los cuales eran absolutamente soberanos ad intra e iguales entre si ad extra, “el poder político

supremo investido en aquel cuyos actos no pueden ser discutidos por otra voluntad humana",[20] ya fuera en tiempos de guerra o en tiempos de paz.

Para el jurista y politólogo alemán Herman Heller su noción de soberanía esboza una manera distinta de percibir el derecho internacional, exponiendo la primacía del derecho nacional, una "facultad del Estado para crear y garantizar el derecho positivo".[21] Afirmando que: cada instancia decisoria creada convencionalmente, un tribunal o una instancia arbitral o una mediación política, tiene como límites fijos la soberanía de los estados delegantes. El estado que no se ha sometido convencionalmente a una instancia decisoria es el único que decide, por sí y ante sí, dentro del marco de las normas jurídicas fundamentales, cuáles son los límites de su actividad.

Para el filósofo, profesor y jurista italiano Giorgio Del Vecchio la soberanía es "un IMPERIUM sul territorio e sulla popolazione". La soberanía está implícita en la naturaleza del Estado, ya que si éste no tuviera una supremacía real sobre los individuos que lo componen dejaría de ser Estado.

Esta soberanía, a la que correlativamente responde en los ciudadanos un deber jurídico general de subordinación y acatamiento, proviene radicalmente de la voluntad de los ciudadanos. "Lo Stato e, insomma, la sintesi delle volonta e dei diritti individuali; e il momento ideale di convergenza di questi diritti in una suprema expressione potestativa".[22]

Para la presente tesis, se han retomado las ideas de Norberto Bobbio, nociones que son consideradas afines para explicar las inquietudes sobre el espionaje electrónico en México.

---

[20] "Hugo Grocio", [en línea], 03 de septiembre de 2017, en https://archivos.juridicas.unam.mx/www/bjv/libros/6/2698/11.pdf

[21] "Soberanía y derecho internacional en el pensamiento jurídico de Weimar", [en línea], 03 de septiembre de 2017, en http://www.derecho.uba.ar/investigacion/investigadores/publicaciones/vita-soberania-y-derecho-internacional-en-el-pensamiento-juridico-de-weimar.pdf

[22] "El Derecho Natural en Giorgio", [en línea], 03 de septiembre de 2017, en https://books.google.com.mx/books?id=ebyyd7UUGewC&pg=PA68&lpg=PA68&dq=giorgio+del+vecchio+la+soberania&source=bl&ots=6m0U29ru-d&sig=MoKeWS18csH6qrT4hn5dBubC7YY&hl=es&sa=X&ved=0ahUKEwiosemSoYrWAhXC4yYKHT9eAFUQ6AEIXDAO#v=onepage&q&f=false

Bobbio afirma que:

> En sentido amplio el concepto político-jurídico de soberanía sirve para indicar el poder de mando en última instancia en una sociedad política y, por consiguiente, para diferencia a esta de las otras asociaciones humanas, en cuya organización no existe tal poder supremo, exclusivo y no derivado. Por lo tanto, tal concepto está estrechamente vinculado al poder político; en efecto, la soberanía pretende ser una racionalización jurídica del poder, en el sentido de transformar la fuerza en poder legítimo, el poder de hecho en poder de derecho. Obviamente la soberanía se configura de distintas maneras según las distintas formas de organización del poder que se han dado en la historia de la humanidad: en todas podemos encontrar siempre una autoridad suprema, aunque luego se explique o sea ejercida de maneras muy distintas.[23]

Sin embargo, la injerencia en los asuntos de otra nación a través del espionaje electrónico es una práctica incluida en el accionar de los estados, una práctica que ha tomado gran relevancia en la actualidad y, a su vez, ha desencadenado controversia y una gran polémica en el mundo porque viola el derecho internacional y atenta contra principios que deberían regir las relaciones entre los países como: el principio de no intervención en los asuntos internos de otro Estado establecido en la Carta de las Naciones Unidas,[24] la Resolución 2625[25] de las Naciones Unidas y la jurisprudencia de la Corte Internacional de Justicia.

Además de atentar contra otros derechos humanos como el derecho a la libertad porque no se está libre mientras exista vigilancia de forma ilegítima e irrespetuosa. El derecho a la privacidad y el derecho a la privacidad de información que sin importar a quién vayan dirigidas, son condenables, inaceptables y jurídicamente sancionables por violar el derecho fundamental a la vida privada e intimidad de las personas, y esto resulta más grave cuando se compromete información que podría afectar los intereses de una nación.

---

[23] "Diccionario de Política", [en línea], 22 de mayo de 2017, en http://documents.mx/documents/bobbio-diccionario-de-politica-soberania.html#

[24] "Propósitos y Principio de las Naciones Unidas", [en línea], 28 de agosto de 2017, en http://www.un.org/es/sc/repertoire/principles.shtml

[25] "Resoluciones aprobadas sobre la base de los informes de la sexta comisión", [en línea], 28 de agosto de 2017, en http://www.un.org/es/comun/docs/?symbol=A/RES/2625(XXV)&Lang=S&Area=RESOLUTION

Los alcances del espionaje electrónico en el sistema internacional rompen la confianza entre los estados y desatan las crisis diplomáticas, hechos que deberían ser considerados para la creación de un acuerdo de principios jurídicos que responda a favor de intereses superiores. En donde la soberanía de un país no se base en una acción que sea en detrimento de otra nación soberana. En donde el derecho a la seguridad de las naciones se garantice sin violar los derechos humanos y civiles de otros.

1.3 Antecedentes y concepto de seguridad nacional

La seguridad nacional también posee como referente principal al Estado porque es quien asume la responsabilidad de proteger a sus ciudadanos mediante el sometimiento a este. Así, la seguridad de los ciudadanos está garantizada cuando la propia seguridad del Estado también lo está.

El Estado a través de la seguridad nacional, garantiza la integridad del territorio nacional y sus instituciones, al preservar la legitimidad de los poderes, proteger los intereses nacionales en el sistema internacional, hacer efectiva la soberanía territorial, reducir adecuadamente la dependencia con el extranjero, preservar los valores y asegurar el desarrollo nacional.

Son esta las responsabilidades del Estado que lo deben guiar a actuar de manera legítima y a favor de sus ciudadanos, para mantener su prestigio internacional y mantener una cohesión nacional de paz, justicia y seguridad.

De acuerdo a Barry Buzan[26] entre los elementos que conforman la seguridad nacional destacan los siguientes:

1. Interés Nacional: son los valores vitales, la ideología indispensable y los objetivos específicos (permanentes o coyunturales) de un Estado proyectados a nivel nacional e internacional, para lograr mantener un adecuado poder nacional que le permita desenvolverse racionalmente siendo el Estado aquel que procura su protección y consecución.

[26] "Barry Buzan y la teoría de los complejos de seguridad", [en line], 11 de febrero de 2018, en http://www.saber.ula.ve/bitstream/123456789/24849/2/articulo7.pdf

2. Poder nacional: la capacidad de autodeterminación de un Estado, orientado a consolidar, conquistar y preservar los intereses nacionales ya sea por medio de la persuasión o la coerción, empleando todos los medios disponibles en una nación: políticos, económicos, sociales y militares.
3. Amenazas: son los obstáculos de todo orden, de origen interno o externo, material e inmaterial que pueden dificultar o impedir la conquista y el mantenimiento de los intereses de una nación, afectando así su seguridad nacional. Los **problemas de supervivencia** o amenazas de corto plazo (los ciberataques entre Rusia y Georgia, caso desarrollado en capítulo II de la presente investigación). Los **problemas vitales** o amenazas de largo plazo (el robo de identidades asociado a inmigración ilegal, el robo de información de tarjetas de crédito o de los certificados digitales, el blanqueo de dinero actividades realizadas por el crimen organizado). Los **problemas mayores,** sucesos internacionales que pueden convertirse en problemas vitales como el hacking político o patriótico (conflictos regionales, étnicos, religiosos o culturales mediante la de negación de servicios Web en el ciberespacio; China y Japón; Azerbaiyán y Turquía; India y Pakistán, chiitas y sunitas o el conflicto entre árabes e israelíes). Los **asuntos periféricos** afectan las actividades en el extranjero de ciudadanos y corporaciones. Un ejemplo es el espionaje industrial.

La naturaleza dinámica del concepto seguridad nacional genera múltiples interpretaciones, y su campo de acción teórico es tan amplio que debe ser analizado desde una perspectiva flexible y cambiante. Un término complejo porque se construye y adapta de manera circunstancial, modificándose a los contextos históricos, sociales y culturales. Además de las diferentes capacidades de los Estados, su situación interna y la del entorno internacional hacen que la interpretación de las amenazas y los objetivos nacionales sean vistos siempre de diferente manera y motiven así, su formulación constante.

Es decir, la seguridad nacional tiene un significado distinto para todas las naciones o quizá ni siquiera tengan un significado preciso.

La mayoría de los países comprende la seguridad nacional en términos de la preservación de los intereses nacionales, específicamente de una seguridad basada en el poder según los planteamientos realistas. En donde la seguridad nacional nace como una precondición para la existencia ordenada del Estado, como un mecanismo de defensa para garantizar la permanencia y la prosperidad, como un fenómeno social circunscrito al proceso político.

Asimismo la seguridad nacional tiende a confundirse con las labores de inteligencia o con la planeación estratégica; una concepción represiva que se consolida después de la Segunda Guerra Mundial, cuando los Estados Unidos de América redefinieron el uso político de la palabra seguridad, para elaborar el concepto de Estado de seguridad nacional. Este concepto se utilizó para designar la defensa militar y la seguridad interna, frente a las amenazas de revolución, la inestabilidad del capitalismo y la capacidad destructora de los armamentos.[27]

El desarrollo de la visión contemporánea de seguridad nacional ha estado determinado por este origen y fue influenciado por la estrategia estadounidense de contención. El paradigma bipolar, propio de la Guerra Fría, le dio sentido y la desconfianza entre las naciones le proporcionó su dinámica. Con la generalización del uso de esta categoría política, el plano militar se convirtió en la base de las relaciones internacionales.

Con el fin de la Guerra Fría se creyó que llegaría una era de estabilidad, cooperación y menos amenazas a la seguridad mundial. También se pensó que la tendencia de disminución de la importancia de los Estados nacionales y su mayor interdependencia fortalecerían las decisiones multilaterales para beneficio de la humanidad. Esta visión se cumplió, en buena medida, para los países más prósperos. No obstante, para los países menos favorecidos, las circunstancias

[27] Tocora Fernando, “Política Criminal en América Latina, Seguridad Nacional y Narcotráfico”, p. 183-185.

eran distintas, la idea de alcanzar su soberanía plena dentro de un nuevo orden mundial se derrumbó y la inestabilidad continuó marcando a sus sociedades.

Renacieron antiguos conflictos regionales, étnicos, religiosos y nacionalistas. Además, algunas de las decisiones multilaterales que se tomaron fueron para realizar intervenciones en los países más inestables, con respaldos legitimadores como el de las Naciones Unidas.

En este nuevo contexto, las amenazas a la seguridad se perfilaron como problemas sociales de orden trasnacional y no como conflictos entre los Estados. El narcotráfico, la corrupción, el terrorismo, la violación de los derechos humanos y la destrucción del medio ambiente son ejemplos de estas nuevas amenazas. Con ellas apareció la tendencia a la privatización de las guerras, principalmente en los países inestables. Además, Estados Unidos se erigió como el centro del poder militar, aunque hubo ensayos multilaterales de cooperación excepcionales, como el de la Guerra del Golfo, que respondieron más a razones económicas que a necesidades estratégicas. Así mismo, la prosperidad económica alejó aún más a los países en vías de desarrollo de aquellos que basan su crecimiento más en la desregulación financiera internacional que en su gran capacidad tecnológica y productiva.

La tensión entre quienes confiaban en la cimentación de la estabilidad y aquellos que veían en la incertidumbre el sello de la posguerra fría, duró poco más de una década. Los trágicos sucesos del 11 de septiembre de 2001 mostraron un punto de inflexión. Las naciones que aceptaban la visión de estabilidad y confiaban en una seguridad eterna resguardada por un gran desarrollo tecnológico que fortalecía a los organismos, militares, policiales y de seguridad no existían.

En el actual contexto internacional, con el surgimiento de nuevas amenazas, el paradigma de la seguridad nacional se encuentra en una etapa de transición y redefinición, en la que se busca aportar los elementos esenciales para entender la naturaleza de los nuevos retos, su impacto y manera de enfrentarlos de manera integral y estratégica, más que de manera aislada y coyuntural. Así, el nuevo paradigma de la seguridad nacional debe orientarse más solución de las

causas que de los efectos, enfatizando una visión estructural, en la que se articulen diversas realidades (sociales, económicas, de desarrollo y seguridad, entre las principales).

Dentro del nuevo paradigma de seguridad nacional destaca también la interconexión de distintas empresas, esfuerzos, fenómenos, organizaciones, dentro de redes de interés e influencia, con una gran capacidad de movilización y convocatoria, que son potenciadas en la era de las Tecnologías de la Información y Comunicación.

El Programa de las Naciones Unidas para el Desarrollo en su Informe Mundial sobre el Desarrollo Humano 1994[28]sustenta la seguridad como multidimensional por la naturaleza de las nuevas amenazas a la sociedad internacional y en las siete esferas de la seguridad humana (económica, política, personal, ambiental, social, alimentaria y de salud), condiciones de estabilidad favorables para el desarrollo de los individuos, un país o de la comunidad internacional.

José Thiago Cintra, en su libro "Seguridad Nacional, Poder Nacional y Desarrollo" define la seguridad como: "una noción de garantía, de protección o tranquilidad frente a amenazas o acciones adversas a la persona humana, a instituciones o a bienes esenciales, ya sean existentes o pretendidos".[29]

El actual Plan Nacional de Desarrollo 2013-2018, menciona que:

> El concepto jurídico de Seguridad Nacional condensa una serie de objetivos e intereses estratégicos nacionales, tales como la protección de la nación mexicana frente a las amenazas y riesgos; la preservación de la soberanía e independencia nacionales y la defensa del territorio; el mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno; la preservación de la unidad de las partes integrantes de la Federación; la defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional; y el desarrollo económico, social y político del país como ejes en la preservación de la democracia.

---

[28] "Informe sobre el desarrollo humano 1994", [en línea], 28 de febrero de 2018, en http://hdr.undp.org/sites/default/files/hdr_1994_es_completo_nostats.pdf

[29] "Seguridad Nacional, Poder Nacional y Desarrollo", [en línea], 26 de febrero de 2018, en https://asiapacificoydelsurfesaragon.wikispaces.com/file/view/Cintra.pdf

La política integral de seguridad nacional del Estado Mexicano, se orienta a todos aquellos factores que vulneran al elemento humano del Estado. Al ampliar el concepto de seguridad nacional en el diseño de las políticas públicas, se atienden problemáticas de naturaleza diversa a las estrictamente relacionadas con actos violentos que vulneran los derechos fundamentales de la población mexicana. Además de restablecer la tranquilidad y seguridad de los ciudadanos, enfrentando toda manifestación de violencia y delincuencia de alto impacto, se combate a la pobreza, se vela por una educación con calidad, se previenen y atienden enfermedades, se da equilibrio ecológico y protección al ambiente, de este modo, la seguridad nacional adquiere un carácter multidimensional.[30]

Para la presente tesis se retomará la concepción mexicana de seguridad nacional, en la Ley de Seguridad Nacional de 2005, que en su artículo 3° establece que:

Para efectos de esta ley, por seguridad nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conllevan a:

La protección de la nación mexicana frente a las amenazas y riesgos que enfrenta nuestro país;

La preservación de la soberanía e independencia nacionales y defensa del territorio;

El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;

El mantenimiento de la unidad de las partes integrantes de la federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

La defensa legitima del Estado mexicano respecto de otros Estados o sujetos de derecho internacional, y

La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes.[31]

En una visión integral de la seguridad nacional se debe reconocer que los objetivos e intereses de seguridad y protección de otros Estados son compartidos o al menos compatibles con los propios, una búsqueda que implica concebir y

[30] "Plan Nacional De Desarrollo 2013-2018", [en línea], 23 de febrero de 2018, en http://www.snieg.mx/contenidos/espanol/normatividad/MarcoJuridico/PND_2013-2018.pdf

[31] "Ley de Seguridad Nacional", [en línea], 22 de abril de 2016, en http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf

participar en la seguridad internacional, la cual debe ser parte de un proceso continuo, cíclico y responsable, buscando en todo momento consolidar las condiciones mínimas para la estabilidad y dinámica internacional y en consecuencia de la estabilidad de nuestra nación.

Ha sido en nombre de la seguridad nacional que, algunos estados han pasado por alto cualquier noción sobre los derechos humanos en la era digital. La vigilancia masiva en las comunicaciones, independientemente de la nacionalidad o la ubicación de las personas, se ha convertido en un hábito en lugar de una medida excepcional, hábito que ha mermado notablemente nuestros derechos en Internet por temor a una vigilancia excesiva.

La responsabilidad de los gobiernos, es demostrar que sus prácticas son necesarias y proporcionales a sus objetivos de seguridad, sin embargo, el derecho a la privacidad de las personas es constantemente quebrantado por propósitos, tanto legítimos como ilegítimos, dentro y fuera de internet, ya sea para frustrar amenazas de seguridad o para identificar una voz particularmente crítica contra la política gubernamental.

El aspecto más preocupante es, que algunos estados siguen argumentando que no tienen la obligación legal de proteger la privacidad de nadie fuera de sus respectivos territorios, olvidando que nuestro mundo está interconectado, es insostenible argumentar que el derecho a la privacidad termina en la frontera mientras que la vigilancia carece de ellas.

Sin duda, existen razones legítimas de secretismo al abordar amenazas de seguridad nacional. Sin embargo, esos poderes deben estar sujetos a la supervisión para evitar las extralimitaciones y el abuso, incluso mediante órganos judiciales y parlamentarios.

Permanece en la agenda internacional desarrollar normas, directrices y establecer instituciones para asegurar que la privacidad siga teniendo sentido en la era digital. Aunque el desarrollo de una normativa global es solo un primer pasó. A medida que se desarrollan nuevas capacidades de vigilancia y los Estados

abordan nuevas amenazas son imprescindibles el continuo escrutinio público y la implementación nacional de normas globales.

Ahora la responsabilidad recae sobre los parlamentos y los legisladores de todo el mundo para que examinen las prácticas de vigilancia y evalúen sus costos y beneficios tangibles con más atención y de manera pública dentro de un marco de derechos humanos.

1.4 Derechos humanos

Fueron las revelaciones hechas por Edward Snowden en junio de 2013, en donde se demuestra el alcance masivo y global del programa de vigilancia de la Agencia de Seguridad Nacional de los Estados Unidos con la participación de otros gobiernos, para llevar a cabo operaciones de marcado interés militar, entre ellas, el espionaje electrónico. Todo esto sin ningún control legal significativo ni supervisión, y sin tener en cuenta los derechos de millones de personas que no eran sospechosas de haber cometido ningún delito.

La premisa que provocó una toma de conciencia en el siglo XXI para prevenir el desvanecimiento de las fronteras entre lo público y lo privado, fueron los avances de Internet y la inserción, cada vez mayor, en las redes sociales y plataformas de nuestra cotidianidad. El debate entre empresas que temen una regulación y los defensores de la privacidad que temen la intrusión del gobierno.

Razonamientos que nos plantearon nuevas interrogantes por las severas implicaciones que tienen sobre los derechos humanos de todos los individuos: ¿cuál es la justificación para realizar una vigilancia masiva?, ¿cuál es la competencia de las autoridades en los casos de ataques cibernéticos o la defensa de la infraestructura crítica de una nación?, ¿existe una verdadera protección de nuestra privacidad por parte de los gobiernos y las empresas involucradas en actividades de espionaje electrónico?

En la página web de la Oficina del Alto Comisionado de Naciones Unidas sobre Derechos Humanos define:

Los derechos humanos son derechos inherentes a todos los seres humanos, sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua, o cualquier otra condición. Todos tenemos los mismos derechos humanos, sin discriminación alguna. Estos derechos son interrelacionados, interdependientes e indivisibles.

Los derechos humanos universales están a menudo contemplados en la ley y garantizados por ella, a través de los tratados, el derecho internacional consuetudinario, los principios generales y otras fuentes del derecho internacional. El derecho internacional de los derechos humanos establece las obligaciones que tienen los gobiernos de tomar medidas en determinadas situaciones, o de abstenerse de actuar de determinada forma en otras, a fin de promover y proteger los derechos humanos y las libertades fundamentales de los individuos o grupos.[32]

El Servicio Profesional en Derechos Humanos[33] indica que las características de los derechos humanos son:

- **Imprescriptibilidad:** no se pierden por el simple paso del tiempo.
- **Inalienabilidad:** no se pueden vender, ni transmitir la posesión o el uso de ninguna forma.
- **Indivisibilidad:** se relacionan con el rechazo a cualquier posible jerarquización. Los Estados no están autorizados a proteger y garantizar una determinada categoría de derechos humanos en contravención de otra, sino que todos éstos merecen la misma atención y urgencia.
- **Interdependencia:** Enfatiza la interrelación y dependencia recíproca entre las diferentes categorías de derechos.
- **Integralidad:** Enfatiza la relación de los derechos en los actos violatorios, cuando se violenta un derecho es muy probable que también otros sean vulnerados.
- Tiene carácter absoluto: Los derechos humanos pueden desplazar cualquier otra pretensión moral o jurídica, colectiva o individual, que no tenga el carácter de derecho humano.

---

[32] "¿Qué son los derechos humanos?", [en línea], 07 de mayo de 2017, en http://www.ohchr.org/SP/Issues/Pages/WhatareHumanRights.aspx

[33] "En 2005, la Comisión de Derechos Humanos del Distrito Federal instauró el Servicio Profesional en Derechos Humanos (SPDH) para garantizar la profesionalización del personal de la institución que realiza las labores de defensa, promoción y estudio de los derechos humanos, a fin de asegurar una atención integral a la ciudadanía. Uno de sus objetivos fundamentales consiste en desarrollar una estrategia de alta formación en derechos humanos, con reglas claras y transparentes que permitan a sus integrantes mejorar su desempeño institucional en concordancia con lo establecido por los más altos estándares internacionales en la materia."

- **Universalidad:** Los derechos humanos se adscriben a todos los seres humanos.

En palabras del doctor en Derecho, Jorge Carpizo McGregor, los derechos humanos revisten características que los singularizan; éstas son:

- **Universalidad:** significa que todo ser humano posee una serie de derechos con independencia del país en que haya nacido o habite. Como consecuencia, éstos derechos son exigibles por todos los seres humanos en cualquier contexto político, jurídico, social, cultural, espacial y temporal.
- **Historicidad:** se refiere a tres aspectos diversos:

  a) la evolución de la civilización; el reconocimiento de los derechos humanos y de su contenido es, en buena parte, resultado de la historia universal y de la civilización y, en consecuencia, sujeto a evolución y modificación.

  b) nuevos problemas, necesidades y retos; se precisan derechos por la existencia de necesidades que con anterioridad no existían o protegerlos no revestía mayor importancia. Por ejemplo, es claro que el derecho a la intimidad y privacidad adquiere un significado diferente con la aparición del telégrafo y el teléfono, más aún con los nuevos medios electrónicos de comunicación como el internet. Hasta hace algunas décadas, ésos no eran problemas o no presentaban la gravedad que en la actualidad tienen en muy diversos países, y varios de esos problemas afectan al mundo entero y con la amenaza de que si no se toman las medidas necesarias y urgentes, la afectación de derechos puede volverse crítica para la gran mayoría de la población mundial.

  c) el contexto social y cultural de cada país. Existe un margen de discrecionalidad y de ajustes al reconocer los derechos humanos en una Constitución o ley, siempre y cuando no se violen los derechos universalmente reconocidos y los cuales el Estado está obligado a respetar por medio de tratados internacionales que ha ratificado o por el *jus cogens*.
- **Progresividad:** implica que su concepción y protección nacional, regional e internacional se va ampliando irreversiblemente, tanto en lo que se refiere al número y contenido de ellos como a la eficacia de su control. A su vez, esta característica implica la irreversibilidad de los derechos. Una vez reconocidos no es posible desconocerlos porque, sería un contrasentido, un absurdo que “lo que hoy se reconoce como un atributo inherente a la persona, mañana pudiera dejar de serlo por una decisión gubernamental”.
- **Aspecto protector:** se ampara a toda persona humana.

- **Indivisibilidad:** implica que todos los derechos, ya sean civiles, políticos, económicos, sociales, culturales o de solidaridad forman una unidad. Desde luego que no se puede conducir una existencia humana si se carece de libertad, igualdad y seguridad jurídica, pero éstas no son suficientes si no se cuenta con un nivel adecuado de satisfactores económicos, sociales y culturales, y será muy difícil disfrutar de esos derechos si el país enfrenta una guerra civil o externa.
- **Eficacia directa:** significa que los derechos humanos reconocidos en la Constitución y en los instrumentos internacionales ratificados por un país vinculan obligatoriamente a todos los poderes públicos —Ejecutivo, Legislativo, Judicial y Órganos Constitucionales Autónomos—, así como a autoridades, grupos y personas, y para ello no es necesario que una ley desarrolle los alcances de ese derecho humano, aun en el supuesto de que la Constitución señale la existencia de esa ley. [34]

En la Constitución Política de los Estados Unidos Mexicanos en el Artículo 1º indica que:

> En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece. Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia. Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley. Está prohibida la esclavitud en los Estados Unidos Mexicanos. Los esclavos del extranjero que entren al territorio nacional alcanzarán, por este solo hecho, su libertad y la protección de las leyes. Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las

[34] "Los derechos humanos: naturaleza, denominación y características", [en línea], 19 de febrero de 2018, en https://revistas.juridicas.unam.mx/index.php/cuestiones-constitucionales/article/view/5965/7906

preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.[35]

Por la importancia en el siglo XXI y por ser un referente en la presente investigación nos centraremos en el acceso a internet como un derecho humano y cómo repercute en otro derecho fundamental, como es la privacidad de los individuos.

En el Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión[36] Frank La Rue menciona que: "La única y cambiante naturaleza de internet no sólo permite a los individuos ejercer su derecho de opinión y expresión, sino que también forma parte de sus derechos humanos y promueve el progreso de la sociedad en su conjunto".[37]También destaca el valor de la red "como uno de los más poderosos instrumentos del siglo para aumentar la transparencia en la conducta de los poderosos, acceder a la información y facilitar la participación activa de los ciudadanos en la construcción de sociedades democráticas".[38]

Sin embargo, existen forman en las que se viola este derecho como son:

- Filtrar o bloquear el contenido de Internet.
- Desconectar a los usuarios del acceso a Internet porque viola las libertades de expresión y de acceso a la información de los ciudadanos.
- Ciberataques e inadecuada protección del derecho de privacidad y control de datos.

Esta última como consecuencia de los casos de violación indiscriminada a gran escala del derecho a la privacidad de ciudadanos estadounidenses y no estadounidenses por los programas de vigilancia promovidos por organismos

[35] "Constitución Política de los Estados Unidos Mexicanos", [en línea], 14 de mayo de 2017, en http://www.sct.gob.mx/JURE/doc/cpeum.pdf
[36] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", [en línea], 07 de mayo de 2017, en http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[37] "La ONU declara el acceso a Internet como un Derecho Humano", [en línea], 07 de mayo de 2017, en http://expansion.mx/tecnologia/2011/06/08/la-onu-declara-el-acceso-a-internet-como-un-derecho-humano
[38] "ONU: Internet es un derecho humano", [en línea], 07 de mayo de 2017, en http://archivo.eluniversal.com.mx/articulos/64522.html

gubernamentales de los Estados Unidos de América, en cooperación con el sector privado. Del mismo modo los hackeos que sufrieron los sistemas de las multinacionales PlayStation (Sony),[39] Xbox (Microsoft) y el servicio de correo electrónico de Google.

Acciones que violan la privacidad de todas las personas, un derecho que repercute en nuestra libertad de expresión y asociación con aquellos que elegimos, la toma de decisiones políticas, la práctica de nuestras creencias religiosas, la búsqueda de ayuda médica, el acceso a la educación, decidir a quién amamos y como crear nuestra vida familiar.

El derecho a la vida privada[40] es relativamente reciente. Surge sin ningún antecedente normativo, sin que sea causa de un grave conflicto social que perjudique al Estado, o sin que medie un poderoso interés económico. Su origen son principios generales, pretensiones personales lógicas, la necesidad de tener una completa protección de la persona y las propiedades. Como consecuencia del desarrollo tecnológico, y especialmente del uso de la informática, se manifiesta en el derecho que toda persona tiene al reconocimiento y control del uso y transmisión de sus datos personales.

El primer texto en reconocer el derecho a la vida privada, es la Declaración Universal de Derechos Humanos, de 1948, en su art. 12. Aunque su principal antecedente se encuentra en el artículo "The right to privacy"[41] publicado el 15 de diciembre de 1890 por los abogados estadounidenses Warren y Brandeis.

El objetivo de estos autores era manifestar la necesidad del reconocimiento del derecho a la privacidad. Su definición, "the right to be to alone", el derecho a que lo dejen solo. Trata de proteger un espacio, en este caso íntimo, de la intromisión o injerencia de terceros, de decidir quién puede o no puede participar

[39] "Hackean tienda de PlayStation de Sony en internet", [en línea], 08 de mayo de 2017, en http://www.bbc.com/mundo/ultimas_noticias/2014/12/141208_ultnot_tecnologia_sony_ataque_cibernetico_lv

[40] "Vida privada y protección de datos: un acercamiento a la regulación internacional europea y española", [en línea], 03 de septiembre de 2017, en https://archivos.juridicas.unam.mx/www/bjv/libros/6/2758/10.pdf

[41] "The right to privacy", [en línea], 04 de septiembre de 2017, en http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

de las acciones, de las decisiones, de todo lo acaecido en ese ámbito que pertenece a los sujetos por el mero hecho de ser personas.

Aunque esta definición sigue siendo el máximo referente, también es cierto que el desarrollo de la sociedad, el surgimiento de nuevos intereses, la evolución de los medios y del conocimiento científico y el uso de la informática presentan nuevos riesgos que requieren la oportuna respuesta del ordenamiento jurídico, recordando que el derecho no crea la dignidad de la persona, pero sí asegura su eficacia, garantiza su respeto y posibilita su desarrollo.

Es el derecho que permite definir qué pensamos y quiénes somos; parte fundamental de nuestra autonomía como individuos. Cuando este derecho es aplicado al mundo digital, la privacidad nos aporta límites contra los dispositivos de control indeseados, y con ello, la libertad esencial para el desarrollo personal y el pensamiento independiente.

Sin embargo, la vigilancia masiva global del siglo XXI representa una amenaza para los derechos humanos y algunas naciones han reconocido desde hace tiempo los valores subyacentes al derecho legal a la privacidad: honor, reputación y respeto del hogar y la vida familiar. Los organismos internacionales también han hecho aportaciones considerables como el derecho a la privacidad de todas las personas establecido en el artículo 12 de la Declaración Universal de los Derechos Humanos[42] y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

Artículos en los que se establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, y que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Sin embargo, en nuestros días es difícil conservar la privacidad en Internet porque significa modificar nuestra perspectiva de lo que es Internet; implica entender que surgió como una herramienta de investigación y se convirtió, de

[42] "La Declaración Universal de Derechos Humanos", [en línea], 08 de mayo de 2017, en http://www.un.org/es/universal-declaration-human-rights/

manera involuntaria, en una red global. Implica conocer que su diseño original era garantizar una conectividad sencilla y fiable. Implica dejar de verlo como un espacio privado y percibirlo como uno público, que registra todo lo que hacemos y decimos. Implica comprender que su infraestructura está basada en datos personales, sin duda una desigualdad entre el proveedor y el usuario. Aunado a la desinformación del usuario, que la mayoría de las veces no sabe que sus datos se han recopilados.

Internet, al reducir los costos y eliminar las limitaciones espaciales, ha creado masas de información sobre los individuos y ha hecho cada vez más difícil la creación de límites en torno a esta información socavando el concepto de la privacidad, es decir, la protección de la privacidad no se encuentra integrada en las tecnologías que usamos.

Una razón más de que la privacidad esté en peligro es el deseo de los individuos de publicar su información personal, quizá en algunos casos sin percatarse de la medida en que la han hecho pública. No obstante, sólo por el hecho de que las personas estén más dispuestas o deseen compartir su información personal no significa que también deseen que dicha información se recabe o use para fines comerciales o gubernamentales sin consentimiento previo.

Sin embargo, la jurisprudencia estadounidense fundamentada en la noción de "expectativa razonable de privacidad"[43] se opone a esta idea. Al sustentar que, sólo existe una zona de privacidad garantizada por la Cuarta Enmienda, sí la persona ha actuado conforme a una real expectativa de privacidad y sí tal expectativa la sociedad está preparada para reconocerla como razonable. Es decir, el propósito de la Cuarta Enmienda es proteger a las personas y no simplemente los lugares. Aquello que una persona trata de preservar, como privado inclusive en una zona accesible al público puede ser protegido constitucionalmente, pero sí una persona consiente expone al público, incluso en su propia casa u oficina no es un asunto de protección de la Cuarta Enmienda.

[43] "La expectativa razonable de intimidad y el derecho fundamental a la intimidad en el proceso penal", [en línea], 15 de mayo de 2017, en http://revistas.uexternado.edu.co/index.php/derpen/article/viewFile/2961/2605

Este es el argumento empleado por las empresas en telecomunicaciones para justificar la utilización de nuestros datos, sí una persona comparte voluntariamente su información en el ciberespacio a un tercero, no podría oponerse si se hace pública.

Cada día, millones de personas en el mundo subimos o publicamos material en la red sobre los detalles de nuestras vidas, pensamientos, experiencias y logros, ignorando los peligros que supone para la privacidad, entregar el registro de las actividades cotidianas o los datos personales a los distintos proveedores de servicios (Facebook, WhatsApp, Instagram, Twitter, Snapchat, Tumblr, Flickr, Meetic, Spotify, Youtube, Telegram), sin considerar, si aquellos en quienes depositamos nuestra confianza toman las medidas necesarias de seguridad para proteger nuestra privacidad de las implicaciones que tendrán para nuestra imagen y actividad normal en la red, sí su difusión se hace masiva.

Un recordatorio para toda la sociedad que, una acción en una red pública, como lo es Internet, siempre será una acción pública porque creamos información tangible con respecto a nosotros mismos y nuestros hábitos e intereses simplemente por interactuar en Internet.

Además de no confundir los términos ciberseguridad y derecho a la privacidad. Es decir: la primera hace referencia a "la protección de los servicios e infraestructuras críticas frente a cualquier irrupción, así como la protección de la información contra accesos no autorizados y la privacidad del individuo que tiene de controlar el acceso a su información personal y el uso de la misma, una condición que es posible sólo sí las empresas y los individuos acatan el estado de derecho."[44]

[44] "El debate sobre la privacidad y seguridad en la Red: regulación y mercados", [en línea], 15 de abril de 2018, en https://books.google.com.mx/books?id=oWAV2Bgx7yYC&pg=PA55&lpg=PA55&dq=diferencia+entre+ciberseguridad+y+privacidad&source=bl&ots=2Su-MaCBYx&sig=fZxQQBUhta6gFEhT0OXWuv9Wyjw&hl=es-419&sa=X&ved=0ahUKEwjhgrupkr3aAhWGMd8KHYokB7AQ6AEITDAG#v=onepage&q=diferencia%20entre%20ciberseguridad%20y%20privacidad&f=false

Debemos recordar que el mundo real y el mundo virtual están conectados; nuestras elecciones en el mundo *offline*[45] sobre nuestros amigos, el trabajo, la identidad sexual y las creencias religiosas o políticas se reflejan en nuestros datos y comunicaciones en línea. La exposición no deseada de nuestra información privada puede socavar nuestra seguridad física y moral, porque nos impide desarrollar una identidad personal protegida de la coerción; el objetivo primordial de la privacidad.

Entender lo que significa la privacidad en la era digital implica alcanzar un entendimiento con todas las naciones para "establecer límites a este desarrollo tecnológico tan rápido que estamos viendo"[46] afirmó el portavoz de la Misión Permanente de Alemania ante Naciones Unidas, Christian Doktor.

El 1 de noviembre de 2013, Brasil y Alemania presentaron en Naciones Unidas un proyecto de resolución sobre el derecho a la privacidad en la era digital. En este documento se solicita el establecimiento de mecanismos para garantizar la transparencia y la rendición de cuentas sobre la vigilancia estatal de las comunicaciones. Un texto que motivado por los informes sobre espionaje electrónico global que sufrieron estas naciones así como las afectaciones a una amplia gama de derechos humanos.

También, Alemania fue la pionera en reconocer el "derecho constitucional de la personalidad",[47] o la protección de la integridad y la capacidad de autodesarrollo. El 15 de septiembre de 1983, el Tribunal Constitucional Federal (Bundesverfassungsgericht) de la República Federal de Alemania anulo la Ley nacional del Censo de población, anunciando la autodeterminación informativa como un derecho democrático fundamental. La sentencia tiene el mérito de establecer que es facultad del individuo, derivada de la idea de autodeterminación

---

[45] "Definición de offline o fuera de línea (informática)", [en línea], 16 de mayo de 2017, en http://www.alegsa.com.ar/Dic/offline.php

[46] "Son necesarios límites para proteger la privacidad en el ciberespacio", [en línea], 08 de mayo de 2017, en http://www.un.org/spanish/News/story.asp?newsID=30954#.WRETsUU1-1s

[47] "La protección de datos personales: Derecho Fundamental del siglo XXI. Un estudio comparado", [en línea], 16 de mayo de 2017, en http://www.ejournal.unam.mx/bmd/bolmex120/BMD000012003.pdf

de decidir básicamente por sí mismo cuándo y dentro de que límites procede a revelar situaciones referentes a su propia vida.

Una resolución que ha servido como referente para que la gran mayoría de los países reconozcan una protección a los datos personales de cada individuo. Un enfoque constituido en la creencia de que las personas tienen derecho a acceder y corregir sus datos en manos de diversas instituciones y, en última instancia, tienen el derecho a determinar su uso y eliminación. Un tema que abordaremos en el capítulo II de esta investigación.

Han sido distintas las voces que sostienen que el ciberespacio debería promover la innovación y preservar los derechos, que debería ser una comunidad autogobernada liderada por la sociedad civil con poca necesidad de intervención del gobierno. Sin embargo, esto no ha sido posible, las diferentes formas de pensar y actuar de cada individuo han puesto de manifiesto la necesidad de la intervención de las instituciones garantes de la privacidad.

Instituciones que deberían recordar sus obligaciones de derechos humanos más allá de sus fronteras. Si bien es cierto que, un Estado no puede garantizar los derechos de las personas en el extranjero sin violar la soberanía de otro país. ¿Qué pasa cuando se captura las comunicaciones de millones de personas en el país y en el extranjero?

Recopilar y almacenar grandes cantidades de datos personales confiere el poder de rastrear, analizar y exponer la vida, la seguridad y la dignidad humana de todos nosotros. Un Estado que, sin causa razonable, se apropia en masa de los datos de comunicaciones de los habitantes de otros estados está dañando su seguridad, la autonomía y ejercicio de sus derechos.

El reconocimiento de una responsabilidad global para los Estados con capacidad de vigilancia extraterritorial de respetar la privacidad de todos los que están a su alcance, debería ser una de la mayores preocupaciones de las instituciones existentes porque, si bien las preocupaciones relativas a la seguridad nacional y la delincuencia podrían justificar el uso excepcional y cuidadosamente adaptado de programas de vigilancia, el espionaje electrónico, sin los resguardos

adecuados para proteger la privacidad corre el riesgo de afectar negativamente el disfrute de los derechos humanos y las libertades fundamentales.

1.5 Espionaje electrónico

El espionaje en su origen fue creado para obtener información del enemigo en una situación de conflicto o previo a este. Una actividad que permitía conocer información estratégica sobre la posición, el terreno, las fuerzas y los materiales de un ejército enemigo. Un mecanismo de defensa y supervivencia ante los peligros y amenazas.

Sin embargo, la interceptación de las comunicaciones es tan antigua como la propia existencia de las tecnologías más avanzadas. Es el espionaje, el que se ha visto favorecido por los adelantos tecnológicos, una actividad crucial que ha marcado la historia de la Primera y Segunda Guerra Mundial, escenario de la internacionalización del espionaje por parte de los servicios de inteligencia, convirtiéndolo en una actividad fundamental de la actuación política.

A finales de 1918, cuando la Gran Guerra tocaba a su fin, las invenciones del hombre habían devastado Europa dejando millones de muertos. Por vez primera, los ejércitos dispusieron de flotas aéreas con capacidad para espiar los movimientos y localizaciones del enemigo desde el aire, mediante la fijación de cámaras fotográficas (metralletas de fotos) al fuselaje en aviones de reconocimiento. La revolución de las telecomunicaciones e inteligencia militar permitió la comunicación a larga distancia de forma instantánea. El uso del telégrafo y el código morse fue el comienzo de la comunicación sin barreras de espacio ni tiempo**.** Después surgiría la invención del radio y del teléfono, contribuyendo en la eficiencia de algunos factores cruciales de las guerras, como la logística militar. Para labores de espionaje se registró por primera vez la utilización de máquinas de cifrado para la codificación de mensajes.[48]

[48] "Desarrollo tecnológico bélico durante la 1 ª Guerra Mundial", [en línea], 29 de enero de 2018, en http://www.filmoteca.unam.mx/pages/articulos-revista-toma/desarrollo-tecnologico-belico

La Segunda Guerra Mundial fue el punto definitivo para los servicios de inteligencia en todo el mundo. Las modernas tecnologías militares y de comunicaciones hicieron imprescindible la información precisa y rápida. Algunas de las grandes batallas de esta guerra se entablaron entre los servicios de espionaje y contraespionaje. Algunos de estos casos en nuestros días son parte del conocimiento colectivo como: el código secreto alemán, el ataque por sorpresa de Japón a Pearl Harbor el 7 de diciembre de 1941 supuso un gran éxito de los servicios de inteligencia japoneses y un gran fallo para los estadounidenses. La creación de la CIA, el MI6, la KGB, el Service de Documentation Exterieure et de Contre-Espionage de Francia, el Mossad (servicio de inteligencia de Israel), el Departamento de Asuntos Sociales de China y muchos otros departamentos de inteligencia en una enorme red de espionaje y contra espionaje internacional.

La Guerra Fría fue el perfecto escenario para el espionaje, la vigilancia de la población fue parte de la vida diaria. En especial Alemania Oriental, el servicio de inteligencia del Ministerio de Seguridad monitoreó y registró las actividades de sus ciudadanos, usándola para sofocar revueltas y posibles disidencias.

Los años setenta fueron el marco de un nuevo espionaje, la tecnología convirtió al espacio en el terreno de batalla con mejores sistemas de resolución y captación de información, llamados satélites. En 1971 Estados Unidos puso en órbita por primera vez su Big Bird,[49] un satélite de reconocimiento para recabar información y que estuvo en funcionamiento hasta 1986. El espionaje espacial de los soviéticos se sustentó en los satélites Yantar.

En los últimos tiempos, el sistema de espionaje global ECHELON, cuenta con más de 120 satélites y estaciones de tierra desde la que es capaz de rastrear las comunicaciones a través de internet.

---

[49] "El satélite de vigilancia estadounidense de alto secreto, ahora desclasificado, se muestra públicamente en Virginia", [en línea], 05 de febrero de 2018, en https://translate.google.com.mx/translate?hl=es419&sl=en&u=https://www.washingtonpost.com/blogs/checkpoint-washington/post/top-secret-us-surveillance-satellite-now-declassified-gets-a-public-showing-in-virginia/2011/09/16/gIQAMVssXK_blog.html&prev=search

Del mismo modo que en el pasado, hoy en día el espionaje electrónico es utilizado para mantener las ventajas económicas, culturales, políticas, sociales, además de los considerables avances y desarrollos en las tecnologías de la información y comunicación, hasta el punto de afirmar que a nivel mundial son vitales para la gestión de casi cualquier operación.

Ante este contexto, las sociedades modernas han generado una gran dependencia del ciberespacio. Se han tratado de ignorar, las nuevas amenazas a la discreción, la privacidad y la seguridad, al delegar el control de los procesos de una organización en dichos sistemas. Como consecuencia, en las redes de estas organizaciones se presentan mayores vulnerabilidades, ataques de los que se ignora la procedencia.

De la misma manera, afecta la infraestructura vital de un país, compuesta de instituciones públicas y privadas, que constituyen el sistema nervioso de las naciones. “Desde hace algún tiempo los expertos en privacidad se han venido centrando especialmente en las actividades de creación de perfiles y extracción de datos por parte de las empresas de marketing. Por lo tanto, la cuestión de protección de los datos personales y la privacidad en la era digital se ha convertido en una preocupación fundamental de la política pública, y los Estados se han dado cuenta de la importancia que tiene este problema en sí mismo para la democracia, por no hablar de su papel en fomento del comercio electrónico”.[50]

Como es lógica, esta situación puede ser aprovechada por los servicios de inteligencia de naciones extranjeras, por piratas informáticos, por grupos terroristas, por “el sector privado que utiliza Internet como un instrumento de propaganda porque permite alcanzar la audiencia de millones de personas, favorecer el reclutamiento, la colecta de fondos o incluso la coordinación de acciones a distancia de forma discreta”.[51]

---

[50] Segura Serrano Antonio, Gordo García Fernando, “Ciberseguridad global oportunidades y compromisos en el uso del ciberespacio”, p.60.

[51] Consejo de Europa, Recomendación núm. R (99)5 del Comité de Ministros de los Estados Miembros sobre la protección de la intimidad en internet, Directrices para la protección de las personas respecto a la recogida y tratamiento de datos personales en las “autopistas de la información”, [en línea], 29 de julio de 2015, en

Conforme a la Declaración de Independencia del Ciberespacio,[52] este se considera un nuevo dominio libre y soberano, hasta el punto de ignorar la identidad y determinar la localización física de los participantes porque la comunicación generalmente es anónima o bajo un pseudónimo. Esta situación genera diversas interrogantes: ¿quién gobierna Internet?, ¿pueden o deben aplicarse las leyes de determinado país en Internet?, ¿cómo debe ser gobernado Internet?, ¿por qué debe ser gobernado Internet? y ¿cuáles son las consecuencias de la falta de normas en Internet?

> "Un posible compromiso del progreso tecnológico es facultar a los Estados para hacer valer sus normas relativas a la actividad desarrollada en el ciberespacio".[53] La creación de una regulación en el ciberespacio e instituciones garantes de ellas, son acciones de Estado que contribuirán a una conciencia social y a reducir las actividades delictivas como: "el reconocimiento de sistemas informáticos, la detección de vulnerabilidades en los sistemas para desarrollar herramientas que permitan explotarlas, el robo de información mediante la interceptación de mensajes, modificando el contenido y la secuencia de los mensajes transmitidos, el análisis de datos y el tipo de tráfico transmitido a través de redes informáticas, la realización de ataques para suplantar la identidad IP, la captura de contraseñas y cuentas de usuarios, la conexión de forma no autorizada a equipos, servidores y sistemas informáticos, el envió de malware, el ataque a sistemas criptográficos, el engaño y la extorsión, o la denegación servicios, actividades características del ciberespionaje."[54]

Para la presente tesis los términos espionaje electrónico, espionaje digital o ciberespionaje se utilizarán de modo indistinto con el propósito de incluir las definiciones disponibles del concepto.

Se entiende por espionaje electrónico a: "Obtener, saber o copiar la información confidencial o clasificada de forma no autorizada de un equipo de

---

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/cconsejo_europa/recomendaciones/common/pdfs/Recomendacion_99_5Internet.PDF.

[52] "La Declaración de Independencia del Ciberespacio, cumple 10 años", [en línea], 11 de febrero de 2018, en http://www.lavanguardia.com/internet/20060208/51262741553/la-declaracion-de-independencia-del-ciberespacio-cumple-10-anos.html

[53] Segura Serrano Antonio, Gordo García Fernando, "Ciberseguridad global oportunidades y compromisos en el uso del ciberespacio", p.50.

[54] "El ciberespionaje", [en línea], 15 de febrero de 2018, en https://webcache.googleusercontent.com/search?q=cache:Wp_gzPkZ97YJ:https://dialnet.unirioja.es/descarga/articulo/4330467.pdf+&cd=2&hl=es-419&ct=clnk&gl=mx

destino mediante el uso de sistemas tecnológicos de información y redes para obtener una ventaja militar, política o económica, lo cual nos indica que el perpetrador puede ser de distintas índoles, como son: particulares, es decir individuos, competidores en un mercado determinado, por ejemplo en el mercado comercial, grupos militares, de insurgencia, etc., o gobiernos".[55]

El espionaje electrónico político o industrial ha constituido la mayor amenaza para los países, porque está especialmente dirigida a los sistemas de información de las corporaciones industriales, empresas de Defensa, alta tecnología, automoción, transportes, instituciones de investigación y Administraciones Públicas.

El espionaje electrónico tiene dos clasificaciones: el primer caso es, el espionaje electrónico industrial realizado por organizaciones privadas las que actúan como atacantes. Su objetivo es el lucro derivado de una obtención ilícita de información y, el deterioro intencionado de los sistemas de sus rivales. El segundo caso es, el espionaje realizado por los Estados, mediante sus Servicios de Inteligencia o Departamentos de Defensa con la finalidad de realizar ciberataques hacia otros Estados para obtener información de relevancia económica, geoestratégica o militar.

Todo acto conlleva un conjunto de características que lo definen de forma general, los programas de espionaje electrónico tienen por característica principal el secreto, pero también incluyen algunos detalles únicos como:

- **Ser intrusivos** (atentan contra la soberanía y la seguridad nacional de los Estados. Transgreden los derechos de organismos e individuos).
- **Constar de componentes físicos, virtuales o una combinación de ambos. El diseño y operación son personalizados/especializados para tareas concretas en ámbitos particulares** (son patrocinados generalmente por las agencias de seguridad estales o grandes empresas).
- **Contar con gran capacidad de almacenamiento de datos** (tecnología de punta).
- **Se emplean como transmisores remotos de información para generar nuevo conocimiento partiendo del análisis e integración de información** (empleo, de

[55] "TIC (Internet) y ciberterrorismo – III" [en línea], 23 de marzo de 2017, en https://revista.seguridad.unam.mx/node/2223

"hackers y crackers"[56] para saltear las medidas de seguridad digital a cambio de un pago).[57]

Al aceptar Internet como medio de interconexión global, gran cantidad de tracciones de negocios se realizan de esta forma, por lo que se requieren mecanismos de respuestas rápidas a incidentes de seguridad para evitar que la organización se exponga a pérdidas de respuestas rápidas a incidentes de seguridad para evitar que la organización se exponga a pérdidas irreversibles. Se le denomina un incidente de seguridad informática a cualquier evento que sea considerado una amenaza para la seguridad de un sistema.

Existen diversos tipos de amenazas y seguirán apareciendo cada vez más. Entre las más conocidas tenemos:

- Instalación de software malicioso.
- Acceso sin autorización al sistema o a sus datos.
- Interrupciones indeseadas.
- Denegación de servicios.
- Uso de desautorizado de las bases de datos.
- Cambio en el hardware, firmware o software del sistema.

Es posible clasificar los incidentes de seguridad en dos tipos:

- Incidentes automáticos.
- Incidentes manuales.

Se denominan incidentes automáticos a los incidentes producidos por programas de cómputo tales como virus, gusanos y troyanos. Los incidentes manuales son aquellos en los que de manera intencional se ataca un sistema utilizando, por ejemplo, escaneo de vulnerabilidades, inyección SQL o ingeniería social, aunque bajo ciertas circunstancias, también se pueden realizar de forma automática.

---

[56] "¿Qué es y qué no un hacker?" [en línea], 23 de abril de 2017, en http://www.egov.ufsc.br/portal/sites/default/files/cdn_hacking_v2.pdf

[57] Arreola García Adolfo, "Ciberespionaje: La puerta al mundo virtual de los estados e individuos", p. 30.

Existen diferentes técnicas y programas para la recopilación de información, entre ellas: dialers, adwares, caballos de troya, worms y spywares.[58]

Dialer: programa que utiliza el módem del ordenador para realizar llamadas de tarificación adicional (números de teléfonos internacionales o premium locales) mediante una conexión de marcación sobre Internet, de forma automática y oculta para el usuario. Un ejemplo es el dialer Android.Adware.Mobsqueeze que utiliza nombres como Battery Doctor, Battery Upgrade para engañar a los usuarios haciéndose pasar por un parche para el ahorro de energía en dispositivos Android y así instalarse en el sistema.

Adware (software publicitario): programa gratuito patrocinado mediante publicidad que aparece en ventanas emergentes o en una barra de herramientas en el equipo o navegador. Se utiliza para recopilar información personal, realizar un seguimiento de los sitios web que visita (hábitos de navegación) o incluso registrar las pulsaciones del teclado del usuario en cuestión, actividades potencialmente peligrosas. Entre los programas conocidos que incluyen Adwares se encuentran Alexa, MyWebSearch, FlashGet, Cydoors, Gator, GoHit, Webhancer, Lop, Hotbar, eZula, KaZaa, Aureate / Radiate, RealPlayer, Zango, C2Media, CID, Messenger Plus.

Caballos de Troya o troyanos: programa que accede y controla el ordenador sin ser advertido. Al ejecutarlo crea una puerta trasera (backdoor) que permite la administración remota a un usuario no autorizado. Bajo el nombre de Zeus apareció en 2007, después de un ataque contra el Departamento de Transporte de EE.UU. ha infectado diez millones de equipos y robado cientos de millones de dólares.

Virus o gusanos (worms): programa causante de alteración o borrado de datos, además se propaga a otros ordenadores haciendo uso de la Red, del correo electrónico, etc. Un ejemplo es el gusano de envío masivo de correo Sobig Worm cuya propagación se realiza a todas las direcciones electrónicas

[58] "Troyanos y gusanos: el reinado del malware Análisis de las 100 amenazas más detectadas por ESET en Latinoamérica" [en línea], 22 de abril de 2016 en http://www.welivesecurity.com/wp-content/uploads/2014/01/troyanos-y-gusanos-el-reinado-del-malware.pdf

encontradas dentro de los ficheros de extensiones: .txt, .eml, .html, .htm, .dbx, y .wab.

Programas de espionaje o spyware: programa que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. Es el caso de **CoolWebSearch** al tomar el control de Internet Explorer, la página de inicio y las búsquedas del navegador se enrutan a los sitios web de quien controla el programa (por ejemplo, a páginas pornográficas).

En los últimos años, el aumento de las amenazas vinculadas con la gestión del ciberespacio se ha convertido en un asunto de seguridad nacional para todos los países, porque constituye una de las mayores armas de los Estados y al mismo tiempo uno de sus puntos más vulnerables.

El incremento de los ataques en contra de la infraestructura crítica, los intereses económicos, las redes de información y las capacidades de defensa de naciones específicas, demuestran que existen gobiernos, grupos criminales y organizaciones terroristas dispuestas a explotar el ciberespacio con propósitos hostiles, convirtiéndolo en un nuevo frente de batalla para la geopolítica.

Las brechas de seguridad para recabar información (espionaje electrónico) han superado las fronteras. La captura de información de los servidores de las principales compañías tecnológicas del mundo con apoyo de los servicios de inteligencia de los Estados, amenaza y vulnera los derechos civiles individuales (derechos que no nos han sido otorgados por el contrario son inalienables a nuestra condición humana).

La búsqueda de una visión de la seguridad en donde la privacidad de los ciudadanos de un Estado, constituya un baluarte más de la seguridad nacional y la necesidad creciente de una cooperación internacional ante los problemas relacionados con las tecnologías de la información y el uso del ciberespacio para contar con una legislación supranacional en la materia, que regule y tipifique los delitos en el uso del ciberespacio, bajo la autoridad de la Unión Internacional de Telecomunicaciones (UIT) son el contexto del siglo XXI.

CAPÍTULO 2. POLÍTICAS PÚBLICAS CONTRA EL ESPIONAJE ELECTRÓNICO Y VIOLATORIAS DE LOS DERECHOS HUMANOS

En este segundo capítulo se analizarán las políticas públicas en materia de espionaje electrónico o ciberespionaje ejecutadas en algunas naciones. Se hará énfasis en los casos en donde las consecuencias negativas para los individuos han sido incontrovertibles, mientras que el Estado ha amparado sus acciones en la visión tradicional de seguridad nacional, en donde él continúa siendo el actor principal y el uso de la fuerza legítima su instrumento fundamental.

Lo anterior como consecuencia del conflicto político-jurídico existente entre el derecho a la privacidad y la seguridad nacional. Debido al continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada. Adicionalmente está el propósito actual del desarrollo de la tecnología; considerado un fin o un medio de ataque, llámese vigilancia estatal de las comunicaciones con apoyo de grandes compañías privadas, realizada dentro de las fronteras de un Estado o extraterritorialmente, factor que impide garantizar de manera eficiente las leyes, las normas, las actividades, los poderes, las instituciones y los derechos humanos.

La protección y la garantía de los derechos individuales ante los abusos por parte de actores no estatales (incluidas las empresas), debería ser una responsabilidad de todos los Estados. Diariamente los usuarios de Internet confiamos en las empresas para almacenar y transmitir los detalles de nuestra vida. Conforme a los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos[59] aprobados por el Consejo de Derechos Humanos en 2011 y las directrices de la Iniciativa de Red Global[60] (GNI, por sus siglas en inglés), las empresas de tecnología deben demostrar que están defendiendo a sus usuarios y que tratan de operar con la mayor transparencia.

[59] "La responsabilidad de las empresas de respetar los derechos humanos", [en línea], 29 de junio de 2017, en http://www.ohchr.org/Documents/Publications/HR.PUB.12.2_sp.pdf

[60] "Global Network Initiative; protecting and advancing freedom of expression and privacy in information and communications technologies", [en línea], 29 de junio de 2017, en https://www.globalnetworkinitiative.org/international/Espanol.php

Los cambios generados por la globalización tecnológica han sido de tal magnitud, que han permeado nuestra privacidad hasta el punto de verla amenazada por la huella digital que dejamos diariamente en la mayor innovación tecnológica de las últimas décadas: Internet. Estos aumentos sin precedentes de los flujos de información y comunicación se manifiestan en un escenario carente de garantías de equilibrio entre derechos fundamentales como lo es la privacidad, esencial para la dignidad humana y primordial en una sociedad democrática. Por tal razón su restricción sólo puede estar justificada cuando es prescrita por la ley, es necesaria para lograr un objetivo legítimo y es proporcional al objetivo perseguido.

En su discurso de apertura en el período de sesiones del Consejo de Derechos Humanos, el 9 de septiembre de 2013, la entonces Alta Comisionada de las Naciones Unidas para los Derechos Humanos, Navi Pillay, expresó su preocupación por el amplio alcance de los programas de vigilancia, instó a todos los países a asegurarse de que cuentan con las garantías adecuadas para proteger el derecho a la privacidad y otros derechos humanos, incluso "en los casos en que las preocupaciones de seguridad nacional pueden justificar el uso excepcional y estrictamente delimitado de la vigilancia".

Mantener el delicado equilibrio entre la seguridad y la privacidad en la era digital requiere de la participación de la sociedad civil, la industria y los Estados para evaluar si las leyes y las instituciones son correspondientes con la realidad, en especial con los derechos humanos.

Desde la perspectiva del Sistema Universal de Protección de los Derechos Humanos de Naciones Unidas, dos objetivos son importantes en materia de protección de la privacidad de los individuos. El primero es la Declaración Universal de los Derechos Humanos[61] y, el segundo, el Pacto Internacional de Derechos Civiles y Políticos.[62] En ambos casos se establece que nadie debe ser

[61] "Declaración Universal de Derechos Humanos", [en línea], 16 de abril de 2017, en http://www.acnur.org/t3/fileadmin/scripts/doc.php?file=t3/fileadmin/Documentos/BDL/2001/0013
[62] "Pacto Internacional de Derechos Civiles y Políticos" [en línea], 17 de abril de 2017, en http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia y, además, que toda persona tiene derecho a la protección de la ley contra esas injerencias.

Por otro lado, también los Sistemas Regionales de Protección de los Derechos Humanos protegen este derecho. El Convenio Europeo de Derechos Humanos del Consejo de Europa[63] declara el respeto de la vida privada de los individuos pero establece una serie de excepciones a este derecho entre las que se incluyen la seguridad nacional y la seguridad pública. El Sistema Interamericano de Derechos Humanos, a través de la Convención Americana de Derechos Humanos[64] protege igualmente este derecho.

En el ámbito nacional mexicano, el artículo 16[65] constitucional prescribe ciertas protecciones aisladas sobre aspectos relacionados con la privacidad, como lo es el hecho de que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones sino en virtud de una orden escrita firmada por una autoridad competente. Ni la jurisprudencia ni la doctrina mexicanas ha acuñado algún concepto relacionado con este derecho en el sentido expuesto; a lo sumo, sólo ha recogido los avances alcanzados en otras jurisdicciones.

No obstante, en junio de 2009 se incorporó al mismo artículo constitucional el derecho a la protección de los datos personales y la correlativa facultad que toda persona tiene para acceder, rectificar, cancelar u oponerse a la divulgación de dichos datos. Si bien este derecho, en sí mismo, no agota el derecho a la privacidad (este incluye a aquel), la incorporación constitucional representa un avance importante en el orden jurídico mexicano, pues ha sentado las bases para el desarrollo conceptual del derecho a la privacidad.

---

[63] "Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales" [en línea], 17 de abril de 2017, en http://www.echr.coe.int/Documents/Convention_SPA.pdf

[64] "Convención Americana sobre Derechos Humanos" [en línea], 17 de abril de 2017, en http://www.acnur.org/fileadmin/scripts/doc.php?file=fileadmin/Documentos/BDL/2001/0001

[65] "Artículo 16 Constitucional" [en línea], 27 de junio de 2017, en http://207.249.17.176/Transparencia/XIV%20Transp%20y%20Acceso%20Inform%20Marco%20normativo/Articulo%2016%20Constitucional.pdf

Resulta notoria la existencia de nuevos paradigmas causados por las tecnologías de información y comunicación (TIC), modelos que debemos trascender porque resultan obsoletos para alcanzar nuevas visiones como Estado, se requieren naciones que superen sus limitaciones para buscar principios de seguridad nacional entendidos como la capacidad de proteger y defender a los estados centrada en el bienestar y la salvaguarda de las personas y focalizada en los intereses compartidos por el mundo. Es decir, se necesita un reequilibrio de los instrumentos de defensa, diplomacia y desarrollo a la hora de relacionarse con el mundo.

Para comenzar el análisis de los casos debemos partir del marco de los escándalos enfrentados por el gobierno de los Estados Unidos de América (EUA) por actos de perturbación de los sistemas informáticos o de espionaje electrónico, realizados estos en contra de ciudadanos no sólo de su país sino de todo el mundo, y que fueran provocados por las declaraciones emitidas primeramente por *Julian Paul Assange,*[66] un hacker australiano y fundador del sitio *Wikileaks*.

En abril de 2010 se publicó un video clasificado en el que se puede ver cómo helicópteros Apache estadounidenses abrían fuego contra civiles iraquíes. Al poco tiempo se publicaron los "Diarios de Guerra de Afganistán",[67] con miles de mensajes clasificados que contenían información intercambiada hasta el momento por las tropas estadounidenses. Después surgió el "Irak War Logs",[68] y más tarde los comunicados entre el Departamento de Estado estadounidense con sus embajadas en los que se filtraban secretos diplomáticos, lo que fue denominado como "CableGate".[69]

El caso *WikiLeaks* representa el poder y las consecuencias sobre la información que circula en Internet, un ejemplo de la persecución del Estado contra el individuo.

---

[66] "Un hombre en el centro del huracán", [en línea], 16 de abril de 2017, en http://elpais.com/diario/2010/12/26/domingo/1293339155_850215.html
[67] "Afghan War Diary", [en línea], 16 de abril de 2017, en https://wikileaks.org/afg/
[68] "Iraq War Logs", [en línea], 17 de abril de 2017,en https://wikileaks.org/irg/
[69] "PLUSD The Public Library of US Diplomacy",[en línea], 17 de abril de 2017, en https://wikileaks.org/plusd/

El 7 de diciembre de 2010, el fundador de *Wikileaks*, *Julian Assange* fue detenido y trasladado a la prisión de Wandsworth, Londres. El motivo fue la orden de arresto internacional emitida por Suecia contra *Assange* por los cargos de asalto sexual y violación. Durante su arresto estuvo bajo el régimen de aislamiento, "la detención fue arbitraria e ilegal desde comienzo" señaló el Grupo de Trabajo de Naciones Unidas sobre Detenciones Arbitrarias.[70] El segundo arresto fue domiciliario y por último su confinamiento en la embajada de Ecuador en Londres, desde 2012 (donde aún permanece).

El 19 de mayo de 2017, la Fiscalía de Suecia decidido cerrar la investigación judicial contra *Julian Assange.* El motivo fue el tiempo que duro el procedimiento, es decir, la investigación comenzó en 2010 y el ministerio público sueco retiró los cargos en 2015.

Es de celebrarse, el fallo del panel de expertos de la ONU ante la ilegalidad y la arbitrariedad del acoso penal al que *Julian Assange* ha sido sometido desde fines de 2010. Ciertamente, tal resolución no es vinculante y tampoco obliga a las autoridades de Londres a cesar la persecución, puesto que, existe una orden judicial de detención vigente ante la corte de Westminster. Sin embargo es, una gran victoria para el sistema de Derechos Humanos de Naciones Unidas y para el australiano, porque pone en evidencia a ambos gobiernos como poco respetuosos de sus propias disposiciones legales y de los derechos humanos en general. Además, cabe esperar que las autoridades británicas se den cuenta de lo insostenible de sus posiciones y pongan fin a la persecución contra *Assange*, la cual constituye sin duda el caso más bochornoso de violación a la libertad de expresión y al derecho a la información en una Europa.

Posteriormente, por dos ciudadanos estadounidenses: *Bradley Edward Manning* (*Chelsea Manning*),[71] una mujer transgénero, agente de inteligencia del ejército de Estados Unidos en Irak. En 2010 fue capturada y acusada de entregar

[70] "Expertos de la ONU consideran arbitraria la detención de Julian Assange", [en línea], 27 de junio de 2017, en http://www.un.org/spanish/News/story.asp?NewsID=34385#.WVMNEpI1-1s

[71] "El soldado Manning, condenado a 35 años por las filtraciones a Wikileaks", [en línea], 16 de marzo de 2017, en http://internacional.elpais.com/internacional/2013/08/21/actualidad/1377090640_718161.html

más de 700 mil documentos militares y diplomáticos confidenciales al portal *Wikileaks*, que detallaban los fallos en la guerra en Afganistán e Irak, además de las violaciones de los derechos humanos por parte de soldados estadounidenses (crímenes de guerra).

A raíz de esa filtración, la ex soldado *Manning* fue detenida, sometida a torturas sicológicas y condenada a 35 años de cárcel. La condena fue la mayor de ese tipo impuesta en Estados Unidos y terminaba en 2045. No obstante, el 18 de mayo de 2017, tras siete años de cárcel, abandonó la prisión militar de *Fort Leavenworth*, Texas, cinco meses después de que el ex presidente *Barack Obama* le extendiera una conmutación de pena.[72]

Y *Edward Joseph Snowden,*[73] actualmente refugiado en Rusia, ex agente de la Agencia Nacional de Seguridad (NSA, por sus siglas en ingles), las filtraciones que realizó revelaban como el Gobierno de los Estados Unidos forzó al gigante de las telecomunicaciones, Verizon, a entregarle las conversaciones telefónicas de millones de ciudadanos estadounidenses. La segunda declaración fue para revelar la existencia de un programa llamado PRISM, que recogía información de Internet de las principales compañías de Internet estadounidenses (entre ellas Google, Facebook o Apple).

En el caso *Snowden*, lo más importante fue que una agencia dependiente del Departamento de Defensa de los Estados Unidos (NSA), solicitara estas escuchas y quien creara el sistema de transcripción y búsqueda de información relevante para la seguridad nacional, así como para el uso de estas informaciones como parte de la estrategia de seguridad del país.

Fueron estas filtraciones las que nos permitieron conocer: crímenes de lesa humanidad, actos de corrupción, injerencia de la diplomacia estadunidense en numerosos países –el nuestro, entre ellos–, actitudes inescrupulosas e ilegales de

---

[72] "Chelsea Manning, libre", [en línea], 28 de junio de 2017, en http://www.jornada.unam.mx/2017/05/18/opinion/002a1edi

[73] "Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU.", [en línea], 26 de marzo de 2017, en http://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm

diversos gobiernos y una gravísima sumisión a los dictados de Washington por las naciones que se presentan como libres y soberanas.

Por ello es pertinente cuestionarse sobre las consecuencias de dichas revelaciones, el alcance que tiene el espionaje electrónico y como puede impactar en la vida de los individuos, de una nación y de la comunidad internacional. Tal vez estas actividades que cuestionan la seguridad nacional y principalmente los derechos humanos de los individuos podrían dirigirnos a una búsqueda de leyes y políticas más fuertes, a medida que la vigilancia electrónica se expande y se vuelve universal. Debemos recordar que marcos legales inadecuados crean las circunstancias necesarias para las infracciones arbitrarias e ilegales del derecho a la privacidad en las comunicaciones.

Las leyes nacionales de privacidad se están quedando obsoletas por la falta de actualizaciones, nos dirigimos rápidamente hacia un mundo donde la privacidad desaparece en el segundo en que nos conectamos a Internet o hacemos una llamada telefónica, del mismo modo, las normas internacionales tampoco logran seguir el ritmo de los cambios tecnológicos. La observación general número16[74] del Comité de Derechos Humanos sobre el derecho a la privacidad del artículo 17 no se ha actualizado desde 1988, lo que precede la era digital.

Para avanzar en la comprensión internacional de cómo las nuevas capacidades de vigilancia pueden debilitar la privacidad y otros derechos. Cada país debe asegurar que las personas puedan utilizar estas tecnologías sin temor a intromisiones invasivas y desproporcionadas en su vida privada asegurando la transparencia, la rendición de cuentas y la democracia en el mundo.

[74] "Observaciones generales aprobadas por el Comité de Derechos Humanos", [en línea], 03 de julio de 2017, en https://conf-dts1.unog.ch/1%20SPA/Tradutek/Derechos_hum_Base/CCPR/00_2_obs_grales_Cte%20DerHum%20%5BCCPR%5D.html

2.1. Estados Unidos de América, líder mundial en tecnología de la información

En 1980 se publicó el artículo “The Righ to Privacy”,[75] escrito por Samuel Warren y Louis Brandeis, texto que daría origen al derecho a la privacidad en el sistema jurídico estadounidense. Los autores lo definieron como: “the right to be let alone”, “el derecho a no ser molestado”. Defendiendo un derecho a la privacidad que le otorga a toda persona plena disponibilidad para decidir en qué medida pueden ser comunicados a otros sus pensamientos, sentimientos y emociones.

Aunque ni la Constitución Federal de los Estados Unidos de 1787[76] ni sus Enmiendas reconocen expresamente un derecho a la privacidad, el Tribunal Supremo estadounidense, reconoce como un derecho fundamental a la privacidad en la toma de decisiones de especial relevancia para el desenvolvimiento de la personalidad individual, implícito en el concepto de libertad, a lo largo de una extensa y gradual jurisprudencia en:

- **La Primera Enmienda:** el derecho a la libertad de asociación; que salvaguarda frente a cualquier obligación estatal de revelar la pertenencia a un grupo u organización.
- **La Tercera Enmienda:** en su prohibición de requisar domicilios particulares por los soldados sin el consentimiento de su propietario en tiempos de paz, es otra faceta de la privacidad.
- **La Cuarta Enmienda:** garantiza el derecho del pueblo a estar a salvo de allanamientos y de secuestros irrazonables en sus personas, casas, papeles y pertenencias. Limitando la intrusión del gobierno, incluyéndose no sólo los supuestos de invasión material (*physical trespass*) sino también de vigilancia electrónica.
- **La Quinta Enmienda:** la cláusula protege contra la autoincriminación, permite al ciudadano crear una zona de privacidad (prohíbe revelar

[75] “The Right to Privacy: Samuel D. Warren; Louis D. Brandeis”, [en linea], 03 de julio de 2017, en http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf
[76] “La Constitución de los Estados Unidos de América 1787”, [en línea], 03 de julio de 2017, en https://www.archives.gov/espanol/constitucion.html

información personal) que el gobierno no puede obligarle a renunciar en su perjuicio.

- **La Novena Enmienda**: establece que la enumeración en la Constitución de determinados derechos no será entendida como denegación o disminución de otros retenidos por el pueblo. Es decir, bajo este conjunto de derechos subyace un derecho general a la privacidad amparado por la Novena Enmienda.
- **La Decimocuarta Enmienda**: garantiza el derecho de la persona a adoptar por sí misma las decisiones fundamentales que configuran su vida personal y familiar sin injerencia estatal alguna. En la década de los sesenta surge una jurisprudencia vacilante que tiende a incluir en la zona de privacidad protegida constitucionalmente por el concepto de libertad de la Decimocuarta Enmienda, el interés individual en evitar la divulgación de información personal, la llamada “informational privacy”.

Así, en el sistema constitucional norteamericano el derecho a la privacidad es un concepto amplio, difícil de definir con precisión y que se ha configurado a lo largo de más de un siglo al delimitarse progresivamente los intereses constitucionales que lo integran, esto es, aquellos ámbitos de la esfera privada que tienden a preservar esos intereses de soledad, secreto, autonomía, individualidad, intimidad, desarrollo de la personalidad, libertad de elección en asuntos personales, control de la información personal, así como del sustrato esencial de la inviolable dignidad humana.

No obstante, las publicaciones de los diarios de mayor renombre internacional indican que, el gobierno estadounidense ha y está accediendo a enormes cantidades de datos a través de la interceptación de cables y mediante la solicitud de las comunicaciones de los usuarios (la gran mayoría no son sospechosos de cometer ningún delito) almacenadas por las grandes empresas de Internet y telecomunicaciones (presión de los gobiernos a actores internacionales para monitorear la actividad en línea) que operan a nivel mundial.

El alcance exacto de la recopilación y uso de datos todavía no está claro, los documentos revelados sugieren que las garantías actuales de privacidad han sido violadas miles de veces en los últimos años, provocando el cuestionamiento sobre la idoneidad de los mecanismos de supervisión para garantizar la protección de los datos de todos los usuarios, independientemente de su nacionalidad o ubicación (el gobierno no parece dispuesto a reconocer públicamente los intereses de privacidad de las personas fuera de sus fronteras, ya sea legal o retóricamente).

Como resultado de su historia Estados Unidos ha desarrollado un complejo y frecuentemente subjetivo sistema de salvaguardas para garantizar el derecho a la privacidad en las actividades de vigilancia. "Leyes y prácticas que permiten un menor nivel de protección de la privacidad de las personas que no son ciudadanas o residentes, incompatibles con las obligaciones establecidas en las leyes internacionales",[77] señaló *Joe Cannataci*, actual relator especial de la ONU.

El autor *Michael J. Glennon* en su artículo "National Security and Double Government",[78] señala que: el gobierno estadounidense ha empleado una política constante de seguridad nación, caracterizada por la obtención de información privilegiada sin importar el medio utilizado y la explica mediante la teoría del "*doble gobierno*[79]*. A* su vez, exhibe como el ex presidente Obama dio continuidad a las acciones violatorias del derecho a la privacidad en aras de la seguridad nacional, emprendidas por la NSA con la promulgación de "la Ley de Libertad de los

[77] "Experto de la ONU pide a EE UU que mejore la protección de la información privada", [en línea], 04 de julio de 2017, en http://www.un.org/spanish/News/story.asp?NewsID=37603#.WVxL4RU1-1s

[78] "National Security and Double Government", [en línea], 04 de julio de 2017, en http://harvardnsj.org/wp-content/uploads/2014/01/Glennon-Final.pdf

[79] "Michael Glennon, en su artículo "*Seguridad Nacional y Doble Gobierno"* recurre a la teoría "el doble gobierno" elaborada por William Bagehot para explicar el aparato de seguridad de los Estados Unidos. Glennon expone la estructura del doble gobierno en los Estados Unidos, en donde, la parte *solemne* de la constitución comprende las tres ramas *madisonianas* del gobierno: la Presidencia, el Congreso y el Tribunal Supremo. Las partes eficientes son las llamadas *trumanitas*, por el presidente Harry Truman, que creó el Consejo de Seguridad Nacional, la Agencia de Seguridad Nacional y otros pilares del *complejo militar-industrial* de Dwight Eisenhower. En donde el presidente ejerce escaso control real sobre la orientación general de la política de seguridad nacional. El resultado es una mayor centralización, menos transparencia y un principio de autocracia.", [en línea], 30 de julio de 2018, en http://www.ccoyne.com/Review_of_Glennon.pdf

Estados Unidos (USA Freedom Act), en 2015".[80] Lo que a su vez hace recordar aquello mencionado por Henry Kissinger, secretario de Estado de los EUA, "la seguridad absoluta para una nación es la inseguridad para todas las demás"[81] que bien explica la situación actual de las relaciones de dicho país con el resto del mundo.

El mismo autor especifica que bajo esta estrategia de seguridad nacional no se castiga a aquellos miembros de las agencias de seguridad que espían, torturan o asesinan estadounidenses sin una orden judicial (sin olvidar a los extranjeros que sufren la misma suerte); al contrario, se han incrementado tanto el papel como el número de las operaciones encubiertas; por ejemplo, menciona algunas estas acciones:

a) La ciberguerra contra Irán bajo el nombre del código *Olympia Games.*[82]
b) Las acciones de espionaje para interceptar comunicaciones de líderes extranjeros o el uso de GPS para rastrear personas consideradas como objetivos de seguridad.

---

[80] "En 2015 se promulga la Ley de Libertad de los Estados Unidos (*USA Freedom Act*) como resultado de las denuncias de Edward Snowden contra la NSA por realizar espionaje telefónico, interceptación de datos y la creación de programas cibernéticos para realizar ciberespionaje dentro y fuera de su territorio. Aunque la legislación impone limites a la recopilación masiva de metadatos en las telecomunicaciones de ciudadanos estadounidenses. No obstante, la Ley restaura la autorización para las escuchas telefónicas itinerantes y el rastreo de terroristas.", [en línea], 08 de noviembre de 2018, en https://elpais.com/internacional/2015/06/02/actualidad/1433277585_519201.html

[81] "La seguridad absoluta para una nación es la inseguridad para todas las demás", [en línea], 04 de marzo de 2018, en https://elpais.com/diario/1977/01/21/internacional/222649219_850215.html

[82] "En 2010, Estados Unidos e Israel lanzaron una ciberofensiva contra Irán, bajo el nombre clave de *Olympic Games (juegos olímpicos).* El objetivo era anular el poder y asegurar el control futuro de las operaciones nucleares de Irán, evitando una acción armada de Israel contra este país. El grupo Equation Group de la NSA desarrolló el virus Stuxnet (un virus de tipo gusano para espiar y reprogramar sistemas industriales, como plantas de energía eléctrica o sistemas de procesamiento de deshechos) y sus colegas de Israel se encargaron de inyectar el USB en *Natanz*. El virus reprogramó los ordenadores que controlaban las centrifugadoras usadas para enriquecer el uranio y hacía que estas máquinas enviasen datos de funcionamiento normal, mientras se implementaban una serie de rutinas destructivas. Una de ellas producía el aumento de velocidad en el centrifugado hasta que los componentes del sistema explotasen. El ataque fue un éxito pudo retrasar hasta en dos años el programa nuclear de Irán. Lo más importante del virus informático (*Stuxnet) fue* demostrar que se podía alterar los sistemas mecánicos de cualquier equipo que esté controlado por un software", [en línea], 26 de julio de 2018, en https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?hp

c) Las atribuciones infinitas que tienen los agentes del FBI para hacer entrevistas secretas, plantar informes y hurgar en bases de datos comerciales y gubernamentales de otros estados bajo la máscara de estar en busca de aquellos actores que atentan contra la seguridad nacional de los EUA, sean nacionales o extranjeros.

A continuación, se describen los principales programas creados por la NSA durante el mandato del ex presidente Barack Obama, para ejemplificar el espionaje cibernético fuera del territorio estadounidense:

- **Bullrum:** Romper la encriptación, codificación de Internet y comunicaciones que resguarda la seguridad del comercio electrónico y los sistemas bancarios, así como de información sensible.
- **Prism:** Multidetección de información en redes digitales; espionaje industrial.
- **Marina, Mainway, Pinwale y X-Keyscore:** Bases de datos, red de Internet y computadoras; han servido de recolección de fotografías e identificación de individuos en lugares públicos (reconocimiento visual).
- **Promis (Prosecutors Management Information System):** Conjuntar datos de diferentes fuentes en un solo documento, sobre un individuo en específico; creado para realizar investigaciones criminales; después el programa fue adaptado para espiar.
- **Turbine:** Para manejo de implantes automáticos digitales para la recolección de inteligencia y “ataques activos”.
- **Genie:** Recopilar datos de forma masiva o realizar ataques combinados; busca explotar los sistemas extranjeros; el plan en 2013 era que Genie tuviera acceso remoto a un total de 85 000 dispositivos colocados en espionaje alrededor del mundo.

El propósito de esta investigación es identificar el marco regulatorio, en donde se sustentan las actividades de espionaje electrónico realizadas por Estados Unidos, en favor de su seguridad nacional.

Por tal razón, el siguiente listado es una breve reseña de las principales leyes relacionadas con la temática analizada y no un análisis jurídico profundo:

a. *Ley de Espionaje de 1917 (Espionage Act de 1917).*[83]

Condena las acciones realizadas para obtener o proporcionar información, relacionada con los sistemas de defensa nacional a alguna persona o grupo de personas que no hubieran sido autorizadas para tenerla. En 1961, se realiza una importante modificación para otorgarle autoridad extraterritorial.

En el siglo XXI, las últimas imputaciones se relacionan con la retención o proporción de información clasificada a los miembros de los medios de comunicación. Por ejemplo, los casos Leibowitz,[84] Thomas Andrews Drake,[85] Jeffrey Alexander Sterling,[86] Manning, John Kiriakou,[87] Edward J. Snowden, Reality Leigh Winner.

b. El Acuerdo entre el Reino Unido y los Estados Unidos de América (Security Agreement UKUSA).[88]

Inicialmente fue un acuerdo bilateral de seguridad (EUA y Reino Unido) que con el paso del tiempo se ha convertido en un acuerdo multilateral (Reino Unido, EUA, Canadá, Australia y Nueva Zelanda) para obtener información de las actividades alrededor del mundo. En 1943 fue renovado bajo el nombre de *BRUSA Agreement*, entre las modificaciones incluye el intercambio de personal y regulaciones conjuntas para el manejo del material sensible. La vigilancia y el control de las acciones de las naciones del mundo realizados bajo este acuerdo, se logran a través de la red de espionaje electromagnético o como oficialmente se llama a esta cooperación en inteligencia de señales (SIGINT).

---

[83] "The Espionage Act de 1917", [en línea], 08 de noviembre de 2018, en http://www.digitalhistory.uh.edu/disp_textbook.cfm?smtid=3&psid=3904

[84] "United States vs. Leibowitz", [en línea], 13 de marzo de 2018, en https://www.courtlistener.com/docket/4285776/united-states-v-leibowitz/

[85] "United States vs. Thomas Andrews Drake", [en línea], 13 de marzo de 2018, en https://fas.org/sgp/jud/drake/plea.pdf

[86] "United States vs. Jeffrey Sterling", [en línea], 13 de marzo de 2018, en https://law.justia.com/cases/federal/appellate-courts/ca4/11-5028/11-5028-2013-10-16.html

[87] "United States vs. John Kiriakou", [en línea], 13 de marzo de 2018, en https://www.justice.gov/archive/opa/documents/kiriakou-complaint.pdf

[88] "UKUSA Agreement Release 1940-1956", [en línea], 05 de julio de 2017, en https://www.nsa.gov/news-features/declassified-documents/ukusa/

c. Orden Ejecutiva 12333: Actividades de inteligencia de los Estados Unidos (Executive Order 12333).[89]

Extiende las facultades y responsabilidades de las agencias de inteligencia estadounidenses, especialmente autoriza la recolección de información de inteligencia extranjera dentro de territorio estadounidense por parte de la CIA, bajo condiciones especiales, exceptuando en todo momento aquellas que se refieran a la influencia en los procesos políticos de los EUA, de la opinión pública o de los medios. Además, insta a los responsables de las agencias federales estadounidenses a cooperar plenamente con las solicitudes de información de la CIA.

d. Ley de Vigilancia de Inteligencia Extranjera (Foreign Intelligence Surveillance Act, FISA).

Establece los procedimientos para la vigilancia (física y electrónica) y la recopilación de información de inteligencia extranjera entre potencias extranjeras y agentes de potencias extranjeras sospechosos de espionaje o terrorismo hasta por un año, sin la necesidad de contar con una orden judicial. Para tal efecto, los capítulos de dicha ley prevén lo siguiente:

a) Vigilancia electrónica.
b) Registros.
c) Dispositivos de identificación de las comunicaciones de entrada y salida para propósitos de inteligencia.
d) El acceso a ciertos registros de negocios con fines de inteligencia.
e) Obligaciones de información.

La ley FISA es una de las leyes más cuestionadas por su violación a la Cuarta Enmienda y ha sido el principal instrumento legal para llevar ante los tribunales estadounidenses a los presuntos sospechosos de actos de espionaje y terrorismo. Baste como muestra el caso Wen Ho Lee,[90] acusado y arrestado de

[89] "Executive Order 12333", [en línea], 05 de julio de 2017, en https://www.cia.gov/about-cia/eo12333.html
[90] "The making of a suspect: the case of Wen Ho Lee", [en línea], 30 de julio de 2018, en https://www.nytimes.com/2001/02/04/us/the-making-of-a-suspect-the-case-of-wen-ho-lee.html

robar documentos clasificados sobre armas nucleares para la República Popular China. Después de que los investigadores no pudieron probar estas acusaciones, en junio de 2006, recibió 1.6 millones de dólares como indemnización del gobierno federal y de cinco organizaciones de medios por haber difundido su nombre a la prensa, antes de que se presentaran cargos formales contra él.

En 2008, se amplía la autoridad del gobierno para supervisar las comunicaciones internacionales bajo el nombre de Ley de Enmiendas de FISA.

Es importante mencionar que el programa PRISM, creado por la Agencia de Seguridad Nacional estadounidense, responsable del mayor espionaje electrónico de nuestra historia contemporánea, es legal bajo esta ley, al permitir a los funcionarios recolectar el historial de búsqueda en internet, el contenido de mensajes de correo electrónico, la transferencia de archivos y los chats en vivo, es decir, permite la vigilancia de las comunicaciones de todas las personas para salvaguardar la seguridad nacional estadounidense.

En 2015 fue modificada por la aprobación de la Ley de Libertad de los Estados Unidos, la cual, exige que el Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos[91] publique las sentencias más relevantes para establecer precedentes en casos posteriores y fijar parámetros de orientación para permitir o restringir la conducta de vigilancia.

e. Ley de Intercambio y Protección de la Inteligencia Cibernética (Cyberintelligence Sharing and Protection Act of 2011, CISPA, H.R. 3523).[92]

Permite el intercambio de información del tráfico de Internet entre el gobierno estadounidense y las empresas fabricantes y prestadoras del servicio.

El informe del Departamento de Defensa de los Estados Unidos 2016,[93] menciona que Estados Unidos continua llevando adelante programas de vigilancia

[91] "Foreingn Intellingencce Surveillance Court", [en línea], 17 de marzo de 2018, en http://www.fisc.uscourts.gov/

[92] "The Cyber Intelligence Sharing and Protection Act, H.R. 624", [en línea], 06 de julio de 2017, en https://democrats-intelligence.house.gov/sites/democrats.intelligence.house.gov/files/documents/cispaonepager.pdf

a gran escala con fines de inteligencia, además continuó impulsando la extradición desde Rusia de *Edward Snowden*, el denunciante que reveló el alcance de las acciones estadounidenses de vigilancia masiva en 2013.

Adicional a este informe, el Departamento de Defensa cuenta con un área especial llamada Departamento de Estrategia de Defensa para las Operaciones en el Ciberespacio. El mismo Departamento de Defensa cuenta con una Estrategia Internacional para el Ciberespacio,[94] cuyo objetivo es la colaboración con sus aliados de otras agencias internacionales que tengan los mismos intereses dentro del ciberespacio. Esto sin duda nos muestra la importancia que se le da a las relaciones internacionales dentro del ciberespacio por parte del ejecutivo estadounidense.

Como podemos apreciar, Estados Unidos cuenta con un gran desarrollo de políticas en materia de espionaje electrónico que se presenta ante un mundo hiperconectado, donde la red es un elemento crucial y vital para las sociedades más avanzadas.

Para ilustrar los casos de violación al derecho a la privacidad en favor de la seguridad nacional estadounidense, mencionaremos las demandas más controversiales presentadas ante el Tribunal Supremo de los Estados Unidos:

- En el caso Olmstead vs. United States, 277 U.S. 438 (1928),[95] el Tribunal Supremo dictaminó: las conversaciones telefónicas privadas escuchadas electrónicamente, obtenidas por agentes federales sin aprobación judicial y posteriormente utilizadas como evidencia, no constituían una violación de la Cuarta Enmienda ni de los derechos de la Quinta Enmienda del acusado.

---

93 "Informe Mundial 2017: Estados Unidos", [en línea], 16 de abril de 2017, en https://www.hrw.org/es/world-report/country-chapters/298275

94 "The Department of Defense Cyber Strategy", [en línea], 16 de abril de 2017, en https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

95 "Olmstead vs. United States, 277 U.S. 438 (1928)", [en línea], 07 de marzo de 2018, en https://supreme.justia.com/cases/federal/us/277/438/case.html

- En el caso Katz vs. United States, 389 U.S. 347 (1967)[96] el Tribunal Supremo dictaminó a favor de Katz, aplicando el concepto de expectativa razonable para determinar si la actividad del gobierno constituía una intrusión (mencionada en el capítulo uno de la presente investigación).
- En el caso United States vs. Jones, 565 U.S. 400 (2012)[97] el Tribunal supremo dictaminó que al instalar físicamente el dispositivo GPS en la parte inferior del automóvil del acusado, la policía había cometido una intrusión contra los efectos personales de Jones en virtud de la Cuarta Enmienda.

Los tres casos expuestos ante el Tribunal Supremo de los Estados Unidos, demuestran que el conflicto político-jurídico existente entre el derecho a la privacidad y la seguridad nacional dependen en gran medida del contexto en el que se encuentren, es decir, situaciones específicas para un tema amplio y cambiante.

Además, el estudio realizado en 2015 por Pew Research Center[98] indica que: el 54% de los estadounidenses desaprueban que el gobierno recopile información telefónica y de Internet privada para prevenir el terrorismo. Por otro lado, solo el 42% lo aprueba, y los otros no están seguros. Además, el 74% de los estadounidenses dijeron que no deberían tener que renunciar a la privacidad y la libertad por el bien de la seguridad, mientras que el 22% dijo lo contrario. Esto señala que los estadounidenses generalmente favorecen su privacidad personal sobre la seguridad nacional.

[96] "Katz vs. United States, 389 U.S. 347 (1967)", [en línea], 07 de marzo de 2018, en https://supreme.justia.com/cases/federal/us/389/347/case.html
[97] "United States vs. Jones, 565 U.S. 400 (2012)", [en línea], 07 de marzo de 2018, en https://supreme.justia.com/cases/federal/us/565/400/
[98] "Public Perceptions of provacy and Seciritu in the Post-SnowdeN Era", [en línea], 07 de marzo de 2018", en http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

En 2015, el estudio realizado por PEN American Center,[99] demostró: el 85% de los escritores estadounidenses están preocupados por la vigilancia gubernamental de los estadounidenses y el 73% de los escritores nunca han estado tan preocupados por los derechos de privacidad y la libertad de prensa como lo están hoy.

Para el Gobierno estadounidense, la seguridad nacional es lo más importante y los atentados terroristas del 11 de Septiembre, provocaron el incremento de la vigilancia estatal, el monitoreo de los datos de información en Internet e incluso la solicitud expresa del gobierno a las compañías de telecomunicaciones e Internet, para entregar el contenido encriptado de la información de sus usuarios para investigar delitos y posibles amenazas.

Los actos terroristas han generado miedo en la sociedad y el gobierno estadounidense, aunado a los avances tecnológicos (programas de vigilancia masiva), han llevado al surgimiento de un complejo de vigilancia industrial masivo y secreto. Es decir, acuerdos entre el gobierno estadounidense con proveedores de telecomunicaciones para adquirir y compartir información digital sobre los individuos con supervisión judicial mínima o nula.

Estados Unidos al carecer de una Ley General de Privacidad, aplica leyes separadas a sectores específicos. Por tal razón, hace una división entre la vigilancia realizada a los residentes de los Estados Unidos y la vigilancia que se lleva a cabo, casi sin restricción en el resto del mundo.

En teoría, la Cuarta Enmienda de la Constitución estadounidense garantiza el derecho de los ciudadanos estadounidenses a estar protegidos contra los allanamientos e incautaciones ilegales, sin una causa razonable y una orden judicial adecuada. Es decir, si un funcionario en cumplimiento de la Ley obtiene información violando el derecho de privacidad del acusado, esa información generalmente no puede utilizarse en la corte.

---

[99] “Chilling Effects: NSA Surveillance Drive U.S. Writers to Self-Censor”, [en línea], 13 de marzo de 2018, en https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

Por otra parte, la jurisprudencia de la Cuarta Enmienda sostiene que las personas no poseen expectativas razonables de privacidad en sus documentos y efectos, una vez que se transmiten a terceros. No obstante, la mayoría de las telecomunicaciones están almacenadas en servidores de terceros, y el gobierno argumentar que no es necesario adquirir una orden judicial basada en una causa probable para leer los contenidos de los correos electrónicos de un individuo almacenados en línea, porque los correos electrónicos están físicamente en los servidores, posesión del proveedor de servicios de correo electrónico.

Los estándares de recopilación de inteligencia extranjera son más laxos. La Ley de Vigilancia de Inteligencia Extranjera (FISA) autoriza al gobierno a realizar búsquedas electrónicas y encubiertas en el país, si el objetivo de estas búsquedas es información de inteligencia extranjera, de una potencia extranjera o un agente de un poder extranjero.

La derogada Ley Patriótica, aprobada durante la administración Bush y extendida durante la administración de Obama, permitió a las agencias de inteligencia y seguridad de EE. UU. (NSA) interceptar llamadas telefónicas y correos electrónicos de personas supuestamente involucradas en actos terroristas, sin la necesidad de una orden judicial y el programa de vigilancia masiva PRISM denunciado por Snowden demuestran que, en materia de seguridad nacional, las instituciones mantienen una autonomía, independientemente del partido que gobierne.

Actualmente, la Ley de Libertad de Estados Unidos establece los nuevos procedimientos para la recopilación de datos e información en territorios extranjeros y mediante el Tribunal de Vigilancia de Inteligencia Extranjera (FISC), un tribunal secreto dictamina la legalidad de las operaciones de inteligencia. Los defensores de derechos humanos han solicitado constantemente a las autoridades de Estados Unidos, se brinde un juicio justo en tribunales civiles a todos los sospechosos de terrorismo, y que todas las políticas de seguridad nacional estén

en consonancia con las obligaciones en virtud de los derechos humanos y la leyes humanitarias.[100]

Este doble enfoque en la privacidad constata que los Estados Unidos con frecuencia invocan la seguridad nacional para justificar políticas que violan el derecho nacional e internacional por igual.

El 18 de enero de 2018, el actual presidente Donald Trump, firmó la renovación de la Sección 702, que permite a agencias de inteligencia monitorear las comunicaciones de personas extranjeras fuera de Estados Unidos, y lo prohíbe de manera total en el caso de los estadounidenses.

A pesar de la información ya mencionada, el Congreso estadounidense ha manifestado poco interés, por una mayor supervisión de la vigilancia gubernamental nacional o por la restauración de las salvaguardas que prohíben al gobierno recabar las comunicaciones de nacionales y extranjeros, sin una causa probable y una orden judicial.

"Le he dejado claro a la comunidad de inteligencia que —a menos que haya un propósito imperioso de seguridad nacional—no monitorearemos las comunicaciones de los jefes de Estado y de gobierno de nuestros amigos cercanos y aliados",[101] señaló, Obama.

“Dicho eso, yo personalmente he dado instrucciones para solucionar el proceso para revelar identidades desde que asumí la presidencia, y el voto de hoy es sobre monitoreo en el extranjero de extranjeros malos, en territorio foráneo. Lo necesitamos, ¡pónganse listos!”,[102] declaró, Donald Trump.

---

[100] “Seguridad Nacional”, [en línea], 27 de marzo de 2018, en https://www.hrw.org/es/united-states/seguridad-nacional

[101] “El efecto inesperado del discurso de Obama sobre el espionaje”, [en línea], 27 de marzo de 2018, en http://www.bbc.com/mundo/noticias/2014/01/140116_eeuu_obama_anuncio_nsa_analisis_tsb

[102] “Legisladores renuevan programa para espiar a extranjeros fuera de EU”, [en línea], 27 de marzo de 2018, en https://aristeguinoticias.com/1101/mundo/legisladores-renuevan-programa-para-espiar-a-extranjeros-fuera-de-estados-unidos/

2.2 Federación Rusa, una superpotencia de ciberguerra

Para recuperar el prestigio de potencia mundial, tras la caída de la Unión Soviética, una de las primeras acciones que tomó el gobierno de Vladímir Putin al llegar al poder en el 2000, fue reconstituir los aparatos de seguridad de la Federación Rusa. Un ejemplo, es la política estratégica relacionada con el ciberespacio, conocida como la Doctrina para la Seguridad de la información de la Federación Rusa.[103]

Esta doctrina tiene por objetivo prever los principales riesgos y retos para la seguridad de la información rusa. En este documento, se hace alusión a una posible guerra de la información por otras naciones en contra de Rusia. Se hace hincapié en la importancia de las tecnologías de la información para la estrategia militar rusa: "Se espera que el desarrollo por varios estados del concepto de guerra de la información conlleve a peligrosas medidas de acción en las esferas de la información de otros países del mundo, para así interrumpir la normalidad y el funcionamiento de los sistemas de información y telecomunicaciones, pudiendo obtener acceso no autorizado a los recursos de información que tengan almacenados".[104]

Las principales disposiciones de la protección de datos y la privacidad de la Federación Rusa se encuentra en:

a. El Convenio de Estrasburgo para la Protección de las Personas con Respecto al Tratamiento Automático de Datos Personales, ratificado por Rusia en 2005.
b. La Constitución Rusa de 1993.[105]

---

[103] "Putin aprueba una nueva doctrina para la seguridad de información rusa", [en línea], 11 de julio de 2017, en http://rtw24.com/putin-aprueba-una-nueva-doctrina-para-la-seguridad-de-informacion-rusa/

[104] "El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia", [en línea], 11 de julio de 2017, en https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/1222/TFG000913.pdf?sequence=1

[105] "Constitución de la Federación Rusa", [en línea], 10 de marzo de 2018, en https://archivos.juridicas.unam.mx/www/bjv/libros/1/186/4.pdf

En el articulo23: establece el derecho a la privacidad, incluida la privacidad de la correspondencia y el teléfono y otras comunicaciones, para cada individuo.

En el artículo 24: prohíbe la recopilación, almacenamiento, uso y difusión de la información sobre la vida privada de una persona sin su consentimiento.

c. *Ley Federal No. 149-FZ sobre Información, Tecnologías de la Información y Protección de Datos 2006 (Ley de Protección de Datos).*[106]

d. Ley Federal N° 152-FZ sobre Datos Personales 2006 (Ley de Protección de Datos Personales).[107]

   Regula las actividades relacionadas con el procesamiento de datos personales por parte de los organismos del gobierno, por personas jurídicas y físicas, tanto de forma automática, incluso en redes de telecomunicaciones de datos, como manualmente.

La Estrategia para el Desarrollo de la Sociedad de la Información para 2017-2030,[108] establece la prioridad de los valores morales tradicionales y las normas de conducta en el uso de las tecnologías de la información y la comunicación.

El objetivo principal es crear las condiciones para desarrollar la sociedad del conocimiento en Rusia, entre las medidas destaca, el fortalecimiento del control estatal:

- Mejorar los mecanismos para limitar el acceso a la información cuya difusión está prohibida en Rusia por la ley federal y su eliminación;

---

[106] "Ley Federal N° 149-FZ, de 27 de julio de 2006, sobre Información, Tecnologias de la Información y Protección de la Información (en su versión modificada por la Ley Federal N° 222-FZ de 21 de julio de 2014", [en línea], 10 de marzo de 2018, en http://www.wipo.int/wipolex/es/details.jsp?id=15688

[107] "Federal Law of 27 July 2006 N 152-FZ on PERSONAL DATA", [en línea], 10 de marzo de 2018, en https://pd.rkn.gov.ru/authority/p146/p164/

[108] "Strategy for Informatión Society Development until 2030 approved", [en línea], 09 de marzo de 2018, en http://en.kremlin.ru/acts/news/54477

- Mejorar los mecanismos de regulación legal de los medios, así como un medio para proporcionar acceso a la información, que de muchas maneras puede ser atribuido a los medios, pero no lo son (televisión en línea, agregados de noticias, redes sociales, sitios en Internet, Mensajería instantánea);
- Tomar medidas para el uso efectivo de plataformas de información modernas para la difusión de información confiable y de calidad de la producción rusa.
- Garantizar el uso de algoritmos criptográficos rusos y el cifrado en la interacción de las agencias gubernamentales entre ellos y con los ciudadanos y las organizaciones;
- Llevar a cabo acciones coordinadas para conectarse a la infraestructura de información de la Federación Rusa;
- Proporcionar una protección integral de la infraestructura de información de la Federación de Rusia contra ataques de hackers, incluido el uso del estado del sistema de detección.

Las siguientes legislaciones son las más recientes y cuestionadas en la Federación Rusa, consecuencia del endurecimiento de las restricciones al sector de Internet en estos últimos años**.**

a. Ley para proteger datos personales en la red:

Obliga a todas las compañías de Internet a trasladar los datos de ciudadanos rusos a servidores ubicados dentro del país o sus sitios serán bloqueados.

b. Ley de Privacidad en Internet:

Obliga a los buscadores de Internet a eliminar información personal de sus resultados. Los usuarios de Internet tienen el derecho a solicitar la supresión de la información que sea incorrecta o no sea relevante para posteriores acontecimientos o acciones, proporcionando referencias específicas de las páginas web que quieren eliminar y las compañías tienen diez días para cumplir con la petición. Equiparable al derecho a ser olvidado de la Unión Europea, bajo la

cual los buscadores deben eliminar ciertos resultados, cuando se busca el nombre de una persona.

c. Ley Yarovaya:

Modifica leyes de seguridad pública y una ley antiterrorista preexistente. Las nuevas disposiciones otorgan nuevas facultades a las agencias de seguridad, nuevos requisitos para la recopilación de datos y descifrado obligatorio en la industria de las telecomunicaciones.

La legislación considera un delito manifestarse a favor del terrorismo en Internet (cargo utilizado con mayor frecuencia contra los usuarios de redes sociales críticos con la actitud de Rusia en Ucrania), igualmente no informar a las autoridades sobre una posible actividad criminal (atentados terroristas, revueltas armadas, secuestros y otros crímenes). Además, obliga a los proveedores de telefonía e Internet a almacenar grabaciones de todas las comunicaciones durante seis meses y todos los metadatos durante tres años, así como a ayudar a descodificar servicios de mensajería encriptada (WhatsApp, Skype, Facebook Messenger y otros servicios de mensajería instantánea, como por ejemplo Telegram) a los servicios de inteligencia y empresas de seguridad informática.

La directora de programas para Rusia de Human Rights Watch, Tanya Lokshina, señaló al respecto: “esta Ley es un ataque a la libertad de expresión, a la libertad de conciencia y al derecho a la intimidad y da a las fuerzas de seguridad unos poderes irracionalmente amplios”.[109]

d. *Ley que prohíbe el uso de plataformas de mensajería anónima.*

Prohíbe el uso de plataformas de mensajería anónima (Telegram y VPN; redes virtuales privadas), para evitar el anonimato de los usuarios de Internet y el acceso al contenido ilegal. Simultáneamente obliga a los proveedores de servicios a bloquear las páginas que ofrezcan servicios de VPN y otras formas de eludir la censura y la vigilancia en internet. A las aplicaciones de mensajería se les

[109] “El Gran Hermano ruso: el país aprueba una ley que reduce las libertades y la privacidad”. [en línea], 10 de marzo de 2018, en https://www.eldiario.es/theguardian/Gran-Hermano-aprueba-libertades-privacidad_0_531247722.html

exige que verifiquen la identidad de los usuarios y pongan sus mensajes a disposición de las agencias de seguridad.

Por otra parte, Rusia reconoce que la guerra de la información requiere medidas ofensivas y defensivas para garantizar la seguridad de su ciberespacio. Por ello, los servicios militares rusos, junto con expertos del sector de las TIC y de la comunidad académica, han desarrollado un amplio programa de ciberguerra.

El programa ruso de ciberguerra considera que las metas ofensivas deberían ser:

- La planificación de la ejecución de un primer golpe sobre el enemigo (el campo de batalla del futuro comenzará a cambiar cada vez más hacia el área del efecto intelectual).
- El momento óptimo para realizar el ataque. Previamente a este primer golpe, todos los objetivos deben ser identificados (incluyendo los sistemas de información enemigos), se debe negar el acceso enemigo a la información, la circulación monetaria y de crédito debe ser interrumpida y la población debe ser sometida a masivas operaciones psicológicas, incluyendo desinformación. Esto debe ser llevado a cabo con una planificación previa y mediante inversiones a largo plazo para reconocer y penetrar en sistemas enemigos.
- Las "armas software", "armamento de información" (*information weaponry*), armas basadas en código de programación reciben una gran atención en el programa de ciberguerra ruso. La lista de armas incluye virus (que causen la pérdida de datos), troyanos, programas capaces de modificar códigos a través de acceso remoto y destrucción de infraestructuras críticas de forma remota.[110]

Después del conflicto con Georgia en 2008, los rusos analizaron las lecciones aprendidas como: su incapacidad para dominar la opinión pública sobre los derechos y los errores de la guerra. Factor que contribuyó a la creación de las

[110] "Seguridad Nacional y Ciberdefensa", [en línea], 13 de julio de 2017, en http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf

Russian Information Troops (tropas de la información o cibertropas,),[111] un comando totalmente dependiente de las Fuerzas Armadas rusas y cuya principal misión es velar por la seguridad informática nacional. Al respecto el ministro de Defensa Sergei Shoigu declaró: "tenemos tropas de información que son mucho más eficaces y más fuertes que la sección de contrapropaganda anterior".[112]

Las *Russian Information Troops* se crearon en un contexto de guerra física, y por tanto tienen una naturaleza más hostil y ofensiva. Cumple con las necesidades del ejército en cualquiera de sus operaciones militares relacionadas con el mundo de la información. Incluso se crearon unas fuerzas especiales de la información dentro del mismo comando del ejército, dentro de este comando se les prepararía para poder actuar de manera efectiva en operaciones bajo unas condiciones de crisis inmediata.

La información pública apunta a Rusia como una nación cuya capacidad en ciberguerra es una de las más avanzadas entre las naciones técnicamente desarrolladas, un ejemplo de nación altamente involucrada en el desarrollo de su propia capacidad en ciberguerra. Además de ser considera una nación que cuenta con un número basto de expertos y hackers informáticos que la han colocado como una superpotencia cibercriminal (infraestructura que ha traído consigo un incremento en la confianza y el resurgimiento de la economía rusa.). El florecimiento de la potente comunidad de hackers rusos que ha dominado un importante mercado negro donde se puede conseguir los programas más sofisticados para infectar, infiltrar o romper cualquier sistema informático en el mundo fue en la década de los noventa.

En 199 esta comunidad de hackers consiguió comprometer dos millones de ordenadores del Departamento de Defensa de los Estados Unidos, en lo que el

---

[111] "Las cibertropas rusas, entre las mejores del mundo", [en línea], 17 de julio de 2017, en https://es.rbth.com/tecnologias/defensa/2017/01/11/las-cibertropas-rusas-entre-las-mejores-del-mundo_678818

[112] "Russian military admits significant cyberwar effort", [en línea], 17 de julio de 2017, en http://www.bbc.com/news/world-europe-39062663

Pentágono calificó como una campaña de espionaje electrónico ruso, denominada la *Operation Moonlight Maze.*[113]

Así mismo, con base en el conflicto armado entre Rusia y Chechenia (1999 a 2002), el desarrollo y la investigación de los servicios de inteligencia rusos en materia de *ciberguerra* incremento. Desde los primeros años de la Web, las fuerzas pro chechenas y las fuerzas pro rusas trasladaron sus confrontaciones a internet, utilizándolo como una herramienta de difusión de propaganda y noticias inéditas de un frente de guerra, librando una guerra virtual y una guerra terrestre simultáneamente. Las fuerzas pro chechenas consideras pioneras en la difusión de propaganda antirusa, publicaban imágenes (cadáveres ensangrentados para manipular la opinión pública) e información sobre los incidentes ocurridos (ataques a autobuses chechenos y pasajeros asesinados). A medida que avanzaba la tecnología, los internautas observaban transmisiones de videos en donde la milicia chechena emboscaba convoyes de la milicia rusa.

Aunque los funcionarios del Kremlin negaron su participación, admitieron la necesidad de mejorar sus tácticas en el ciberespacio. Desde entonces, se aplicaron ciberoperaciones para impedir que el contenido pro checheno estuviera disponible en el mundo digital, ocasionando como primacía, la "introducción de medidas militares centralizadas de censura" a partir de acciones que conllevaron a la disponibilidad de contenidos en la web.

En el siglo XXI, los colectivos de hackers rusos han tomado como objetivos a los gobiernos o intereses enemigos del Kremlin: la OTAN, la Unión Europea, Ucrania, Estonia, Georgia, Kyrgyzstan, México y Estados Unidos, infiltrados por la misma unidad rusa llamada: Fancy Bear o APT 28.[114]

---

[113] "The hunt for the dawn of APTSs: a 20 year-old atttack that remains relevant", [en línea], 13 de julio de 2017, en https://www.kaspersky.com/about/press-releases/2017_the-hunt-for-the-dawn-of-apts-a-20-year-old-attack-that-remains-relevant

[114] "Cozy Bear and Fancy Bear: did Russians hack Democratic party and if so why?", [en línea], 13 de julio de 2017, en https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc

El conflicto bélico entre Rusia y Georgia por la región de Osetia del Sur es considerado la primera guerra cibernética, ha sido un primer paso hacia una nueva era en la que los ataques virtuales podrían acompañar al fuego real.

El conflicto armado comenzó el 7 de agosto de 2008, y duró hasta el alto al fuego del 15 de agosto, cuando las fuerzas georgianas se retiraron y las fuerzas rusas ocuparon Osetia del Sur y se establecieron temporalmente en algunas zonas no disputadas de Georgia. Durante la semana de conflicto abierto, y las numerosas semanas posteriores de violencia e inseguridad en las zonas controladas por Rusia, murieron cientos de civiles y decenas de miles fueron desplazados. Incluso si estos lamentables hechos no lograran asombrar a la comunidad internacional, Georgia dio a conocer que, los piratas cibernéticos o hackers rusos se dedicaron a bloquear o manipular algunas páginas oficiales del gobierno limitando su comunicación *on- line.*

Expertos estadounidenses en pirateo informático declararon a *The New York Times* que los ciberataques contra Internet en Georgia comenzaron el 20 de julio, y se intensificaron al iniciarse la guerra. Apoyados de un fotomontaje en el que se comparan imágenes del presidente georgiano, *Mijaíl Saakashvili*, con otras de *Hitler* en poses similares sustituyó el contenido original de la web del Banco Nacional. También la página del jefe de Estado fue bloqueada durante días y se cerró el acceso al Ministerio de Exteriores.[115]

"La guerra por el control de Osetia del Sur sólo duró una semana, pero tendrá consecuencias devastadoras para la población civil durante varias generaciones venideras",[116] señaló Rachel Denber, directora para Europa y Asia Central de Human Rights Watch.

Otro ejemplo, sobre cómo la Federación Rusa ha aplicado los nuevos desarrollos tecnológicos, esta vez en un individuo, es el emblemático caso de

---

[115] "Georgia sufre guerra cibernética", [en línea], 19 de julio de 2017, en https://elpais.com/diario/2008/08/14/internacional/1218664803_850215.html

[116] "Rusia/ Georgia: Todas las partes del conflicto de Osetia del Sur en agosto violaron las leyes de la guerra", [en línea], 18 de julio de 2017, en https://www.hrw.org/es/news/2009/01/23/rusia/georgia-todas-las-partes-del-conflicto-de-osetia-del-sur-en-agosto-violaron

violación a la privacidad del editor *Roman Zakharov*, quien presentó un recurso legal contra la Federación Rusa ante el Tribunal Europeo de Derechos Humanos en 2006. *Zakharov* argumento que la legislación nacional de Rusia permitía a los servicios de seguridad interceptar, por medios técnicos (sistema SORM,[117] equipos de vigilancia instalados en las compañías de telefonía móvil), las comunicaciones de cualquier persona sin obtener autorización judicial previa.

El Tribunal Europeo de Derechos Humanos consideró justificado examinar la legislación ante el riesgo de un sistema de vigilancia secreto creado para proteger la seguridad nacional. Sin embargo, constató deficiencias en el marco jurídico como: las circunstancias en que las autoridades públicas de Rusia están facultadas para recurrir a medidas secretas de vigilancia; la duración de tales medidas, en particular las circunstancias en que deben interrumpirse; los procedimientos para autorizar la interceptación, así como para almacenar y destruir los datos interceptados; la supervisión de la interceptación.

Además, la eficacia de las vías de recurso disponibles para impugnar la interceptación de comunicaciones se veía menoscabada por el hecho de que sólo estaban disponibles para las personas que podían presentar pruebas y la obtención de dicha prueba era imposible en ausencia de un sistema de notificación o posibilidad de acceso a la información sobre intercepción.

Por ello, el tribunal llegó a la conclusión de que las disposiciones legales rusas sobre la interceptación de comunicaciones no preveían garantías adecuadas y efectivas contra la arbitrariedad y el riesgo de abuso inherente a cualquier sistema de vigilancia secreta y que era particularmente elevado en un sistema como el de Rusia. En la sentencia de la Gran Sala, en el caso de *Roman Zakharov vs*. Rusia (solicitud nº 47143/06), el Tribunal Europeo de Derechos Humanos sostuvo, por unanimidad, que existía: una violación del artículo 8 (derecho al

[117] "En Rusia, empresas de internet llevan a juicio al Kremlin por vigilancia en línea", [en línea], 11 de julio de 2017, en http://www.elespectador.com/tecnologia/rusia-empresas-de-internet-llevan-juicio-al-kremlin-vig-articulo-620054

respeto de la vida privada y de la correspondencia) del Convenio Europeo de Derechos Humanos.[118]

Por ello, son altamente significativos los datos del último informe de transparencia de Google 2016,[119] en donde se constata que el gobierno ruso solicitó la eliminación de contenido en internet y el 85% de las veces por razones de seguridad nacional. Y de las 13.200 peticiones recibidas por la compañía estadounidense, casi 12.000 eran videos de YouTube (la suma de todas las solicitudes de los demás países del mundo apenas supera las 9.000).

El 19 de diciembre de 2017, el Grupo Internacional de Derechos Humanos Ágora,[120] envió un mensaje electrónico al Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y expresión, *David Kaye*. Solicitando de su asistencia para instar al gobierno ruso a informar sobre el posible bloqueo del acceso a *Telegram* y al cumplimiento de una resolución de la Asamblea General de las Naciones Unidas sobre el derecho a la privacidad y los límites a la vigilancia estatal.

El informe de la Red Internacional de Organizaciones de Libertades Civiles (INCLO),[121] expone la desmesurada interferencia de las autoridades rusas en cuanto a la libertad de expresión y la amenaza del anonimato *on line*. Además expone la preocupación generalizada por el daño que provoca la recopilación de información a la democracia, al debilitar los procesos y las instituciones democráticas en los países en donde estos se dan por sentados e impedir o socavar el desarrollo de las estructuras democráticas en aquellos países que

---

[118] "Case of Roman Zakharov vs Russia (Application no. 47143/06)", [en línea], 12 de julio de 2017, en http://www.statewatch.org/news/2015/dec/echr-russian-secret-surveillance-judgment.pdf

[119] "Informe de Transparencia", [en línea], 10 de marzo de 2018, en https://transparencyreport.google.com/government-removals/by-country/RU

[120] Asociación rusa de profesionales del derecho, especialistas en casos relacionados con la violación sistemática de derechos humanos en todos los estados postsoviéticos, donde el impacto negativo incluye la tortura y asesinato por parte de las autoridades policiales, la muerte de personas en cárceles y colonias penales, el enjuiciamiento y los ataques penales contra activistas de derechos civiles, periodistas y blogueros, [en línea], 08 de noviembre de 2018, en https://www.inclo.net/members/agora/

[121] "Vigilancia y democracia: historias en 10 países", [en línea], 19 de marzo de 2018, en https://www.cels.org.ar/web/wp-content/uploads/2017/06/Vigilancia-y-democracia_INCLO.pdf

recientemente dejaron atrás sistemas más autoritarios y regímenes de vigilancia abusivos.

La controvertida política rusa exhibe las percepciones antagónicas al interior del país. El deseo gubernamental de controlar la información y el mundo digital ingobernable y en ocasiones defendido por los ciudadanos comunes.

El espionaje electrónico realizado por Estados Unidos y denunciado por Snowden en 2013, fue utilizado por las autoridades rusas para emitir medidas represivas en Internet, bajo el argumento de proteger las comunicaciones del ciberespionaje.

La regulación de internet se realizó mediante la aprobación de dos leyes: la *ley de localización de datos,* que obliga a las compañías extranjeras (Facebook, Twitter, Google, etc.) a reubicar sus servidores en territorio ruso, en donde, el estado puede controlarlos. Además obliga a los *bloggers*[122] con más de tres mil seguidores a registrarse en el gobierno y se prohibieron los portales de noticias independientes, todo esto, en nombre de la soberanía digital. Y *la nueva ley antiterrorista* que obligan a los operadores de telefonía móvil y a las compañías de internet a conservar los detalles de conexión (metadata) hasta por un periodo de tres años. Además de conservar el contenido de las comunicaciones (llamadas, mensajes de correo, etc.) Información que estará a disposición del gobierno de manera inmediata para que sea examinada.

2.3. República Francesa, líder europeo en espionaje electrónico

En su origen, el derecho a la privacidad no estaba consagrado en la Constitución de la República Francesa. El ordenamiento jurídico francés consideraba este derecho como: el objeto propio de los estudiosos del derecho natural y de la filosofía del derecho. Son los estudios realizados por *Saleilles* sobre el derecho al nombre y por *Perraut* sobre los derechos de la personalidad y la contribución de

[122] "Persona o conjunto de personas que administran un sitio o red social en internet con el objetivo de entender, informar o vender.", [en línea], 08 de noviembre de 2018, en https://marketingdecontenidos.com/que-es-un-blogger/

una innovadora jurisprudencia,[123] los que dieron pasó a una serie de conceptos abstractos del derecho positivo. Sin embargo, todos estos esfuerzos estaban limitados por la ausencia de normas sobre la privacidad.

Es en 1970 cuando el Estado francés reconoce el derecho a la vida privada en el artículo 9[124] del Código Civil. La ley establece, por otra parte, que se exponen a sanciones penales todos aquéllos que, sin el consentimiento de las personas, atenten a su intimidad consignando o divulgando expresiones desconocidas o fugaces de su personalidad.

Otras normativas de gran relevancia fueron: la Ley Francesa de Protección de Datos de Carácter Personal;[125] la ley n° 2004-801 de 6 de agosto de 2004;[126] el artículo 1316 del *Code Civil*; el Decreto n° 2007-1527 de 24 de octubre de 2007;[127] la Ley n°2008-3 de 3 de enero de 2008;[128] la Ley n° 2008-696 de 15 de enero de 2008;[129] y el Decreto del 7 de abril de 2009.

En el derecho francés, el concepto de vida privada tiene un uso relativamente reciente, algunos componentes esenciales son:

---

123 "La reception des théories juridiques francaises en droit civil québécois", [en línea], 27 de julio de 2017, en https://www.usherbrooke.ca/droit/fileadmin/sites/droit/documents/RDUS/volume_42/42-3-Devinat-Guilhermont.pdf

124 "Article 9", [en línea], 26 de julio de 2017, en https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006419288

125 "La ley francesa de protección de datos de carácter personal", [en línea], 30 de julio de 2017, en https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/ConferenciaTURK.pdf

126 **"**Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1).", [en línea], 30 de julio de 2017, en https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676

127 "Décret n°2007-1527 du 24 octobre 2007 relatif au droit de réponse applicable aux services de communication au public en ligne et pris pour l'application du IV de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.", [en línea], 30 de julio de 2017, en https://www.legifrance.gouv.fr/affichTexte.do;?cidTexte=JORFTEXT000000428279

128 **"**LOI n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs (1)", [en línea], 30 de julio de 2017, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000017785995

129 **"**LOI n° 2008-696 du 15 juillet 2008 relative aux archives", [en línea], 30 de julio de 2017, en https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019198529

- La libertad del domicilio, que comprende, a su vez, el derecho a elegir y mudar de domicilio, el derecho de las personas a utilizar su domicilio según sus conveniencias y el derecho a su inviolabilidad.
- El derecho al secreto.
- El derecho a la inviolabilidad de la correspondencia, que se asocia al anterior.
- El derecho a la protección de las informaciones nominativas, también derivado del derecho al secreto.
- El derecho a una vida familiar normal, y
- El derecho a la vida sexual.

Normativa jurídica internacional vinculante como estado miembro de la Unión Europea:

- El artículo 12 de la Declaración Universal de Derechos Humanos[130] considera que: 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.
- El artículo 8 del Convenio de Europa de Derechos Humanos (CEDH)[131] considera el derecho a la privacidad un derecho fundamental.

Este texto y las sentencias del Tribunal Europeo de Derechos Humanos tienen gran influencia en Francia. Por ejemplo, la Sentencia del Tribunal Europeo de Derechos Humanos, en el caso Huvig vs. Francia.[132]

---

[130] "La Declaración Universal de Derechos Humanos", [en línea], 14 de agosto de 2017, en http://www.un.org/es/universal-declaration-human-rights/

[131] "Convenio Europeo de Derechos Humanos", [en línea], 14 de agosto de 2017, en http://www.echr.coe.int/Documents/Convention_SPA.pdf

[132] "El Sr. Huvig fue acusado de evasión de impuestos. De conformidad con la orden de un juez fue arrestado y sus llamadas telefónicas tanto comerciales como privadas fueron supervisadas y transcritas. La Sentencia del Tribunal Europeo de Derechos Humanos fue que existe una violación del artículo 8 del Convenio de Europa de Derechos Humanos porque la ley de debe determinar el alcance y las modalidades del ejercicio de dicha facultad discrecional con suficiente claridad para facilitar así al individuo la adecuada protección contra la arbitrariedad. La intervención telefónica en el marco de una investigación por fraude, no sirvió como fundamento de la acusación porque no

- El artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea[133] considera que, toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Ante el riesgo del espionaje electrónico que amenaza la privacidad, el gobierno francés ha revisado en profundidad su política de defensa y de seguridad nacional, en los Libros Blancos de los años 2008 y de 2013, no sólo para adoptar estrategias orientadas a prevenir y reaccionar ante el desafío que representan los ciberataques, sino también, el desarrollo de la industria nacional de ciberseguridad.

En el año 2009 se creó la interministerial Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI),[134] autoridad nacional de defensa de los sistemas de información. Dos años después, se publicó la primera Estrategia Nacional de Defensa y Seguridad de los Sistemas de Información de Francia como consecuencia del primer ataque informático con fines de espionaje electrónico (ciberespionaje) contra los ministerios de economía y finanzas.[135]

Por ello, Francia ha privilegiado las Tecnologías de la Información y las Comunicaciones (TIC), sobre todo, en el ámbito de las Administraciones Públicas y en especial por la Ciberdefensa como un componente de vital importancia para la seguridad nacional. En su libro Blanco del año 2013, las autoridades francesas manifestaron su voluntad de elevar sus inversiones en ciberseguridad y ciberdefensa para anular sus dependencias tecnológicas extranjeras al confirmar e identificar la amenaza de sabotaje a infraestructuras críticas. En el año 2014 publicó el Programa Nacional de Ciberseguridad 2014-2017[136] una estrategia que

---

existía un grado mínimo de protección legal.", [en línea], 08 de noviembre de 2018, en http://lawcenter.es/w/file/download/66083

[133] "Carta de los Derechos Fundamentales de la Unión Europea", [en línea], 14 de agosto de 2017, en http://www.europarl.europa.eu/charter/pdf/text_es.pdf

[134] "ANSSI", [en línea], 30 de abril de 2017, en https://translate.google.com.mx/translate?hl=es-419&sl=en&u=https://www.ssi.gouv.fr/en/&prev=search

[135] "El ministerio de Economía francés, víctima de un gran ataque informático" [en línea], 01 de mayo de 2017, en http://www.elmundo.es/elmundo/2011/03/07/internacional/1299480465.html

[136] "Seguridad nacional, amenazas y respuestas",[en línea], 30 de abril de 2017, en https://books.google.com.mx/books?id=qkBsBQAAQBAJ&pg=PT139&lpg=PT139&dq=ciberdefensa+francia&source=bl&ots=1TYC6noWXr&sig=sVLx0saW6CQoBSD6H_t2dgPndCg&hl=es-

manifiesta el reto de convertir a Francia en una potencia mundial en Ciberseguridad.

En Francia, el espionaje electrónico está especialmente dirigido a los sistemas de información de las corporaciones industriales, empresas de Defensa, alta tecnología, automoción, transportes, instituciones de investigación y Administraciones Públicas. Las evidencias presentadas en los diarios internacionales de mayor renombre permiten afirmar que tales acciones han sido llevadas a cabo por Servicios de Inteligencia o Departamentos de Defensa extranjeros, con el propósito de obtener información de relevancia económica, geoestratégica o militar.

El espionaje estadounidense del que fueron objeto los presidentes *Jacques Chirac, Nicolas Sarkozy* y *Francois Hollande*, en el periodo que comprende los años de 2006 a 2016, es una muestra.

De acuerdo a declaraciones del ex jefe de la CIA, *Michael Scheuer*, historiador y profesor de Estudios de Seguridad de la Universidad de Georgetown, en Estados Unidos. El gobierno estadounidense estaba interesado en conseguir información sobre el liderazgo que el ex presidente Sarkozy tuvo en la intervención militar en Libia, además de saber cómo Francia estaba afrontando la crisis económica y la intervención militar en Mali.[137]

El siguiente ejemplo expone el alcance de hackear un sitio web y las consecuencias que puede traer para un *Estado* y para los derechos humanos.

Los ataques terroristas al semanario satírico francés Charlie Hebdo[138] el 7 de enero de 2015, un ataque perpetrado, cuando dos hombres enmascarados y armados con fusiles de asalto entraron en las oficinas de dicho semanario. Dispararon y asesinaron a doce personas e hiriendo a otros once durante el

---

419&sa=X&ved=0ahUKEwiEmfj-sM3TAhWQ14MKHZKUD7k4ChDoAQhLMAc#v=onepage&q=ciberdefensa%20francia&f=false

[137] "Qué es lo que Estados Unidos espía a sus aliados", [en línea], 02 de mayo de 2017, en http://www.bbc.com/mundo/noticias/2015/06/150624_wikileaks_eeuu_internacional_espionaje_por_que_aliados_se_espian_ig

[138] "Charlie Hebdo attack: Three days of terror", [en línea], 30 de abril de 2017, en http://www.bbc.com/news/world-europe-30708237

ataque. Previamente a esta tragedia, en la madrugada del 2 de noviembre de 2011, incluso antes de que la publicación saliera a la calle, debido a que fue presentado de forma anticipada en las redes sociales, la sede del periódico, fue atacada y su sitio web, hackeado.

Un hecho que sería el comienzo de múltiples ataques perpetrados en distintos puntos de París a lo largo de la tarde y la noche del 13 de noviembre de 2015, considerada la agresión más grave y extensa contra la capital francesa desde la Segunda Guerra Mundial. Fue este el contexto que desencadeno los múltiples ciberataques del colectivo informal de ciberactivistas y hackers (*Anonymous*) contra el Estado Islámico.[139]

Después de los Atentados en París,[140] el 13 de noviembre de 2015, el presidente *François Hollande,* declaró que la nación francesa estaba en: "Estado de Emergencia".[141]

Una medida aplicada sólo en situaciones excepcionales, porque implica la reducción de libertades para garantizar la seguridad del país. Se concede al Ministerio del Interior y a los prefectos amplios poderes como: la autorización para realizar registros bajo simples sospechas y arrestos domiciliarios sin la intervención de un juez. Además, se les obliga a las personas sospechosas a identificarse tres veces al día en la comisaría. Una situación cuestionada por las organizaciones de derechos humanos, porque las personas que han sido objeto de estas medidas no son sospechosas de vínculos con el terrorismo.

Los casos recientes de la violación de la privacidad son: el que presentó la Comisión Francesa de Protección de Datos en el que, afirma que el sistema

---

[139] "Anonymus anuncia su mayor ataque informático contra el Estado Islámico", [en línea], 02 de mayo de 2017, en http://tecnologia.elpais.com/tecnologia/2015/11/16/actualidad/1447689267_713343.html

[140] "Atentados en Paris causan 150 muertos", [en línea], 01 de mayo de 2017, en http://www.jornada.unam.mx/2015/11/14/politica/002n1pol

[141] "¿Qué es el Estado de emergencia y por qué Francia lo mantiene 12 meses después de los ataques de París?, [en línea], 01 de mayo de 2017, en http://www.bbc.com/mundo/noticias-internacional-37966286

operativo Windows 10, propiedad de Microsoft,[142] recopila grandes cantidades de información sobre todos sus usuarios. Otro caso, fue el plazo de tres meses que dio La Comisión Nacional de la Informática y las Libertades (CNLI) de Francia a Facebook[143] para que cumpla con la Ley de Protección de Datos, que incluye dejar de almacenar información sobre la actividad en Internet de los usuarios que no tienen cuenta en la red social, así como a transferir las informaciones a Estados Unidos amparándose en el Acuerdo Safe Harbourn[144] (acuerdo derogado desde 6 de octubre de 2015[145]) a pesar de que el Tribunal de Justicia de la Unión Europea declaró ilegal este acuerdo. Un caso en el que las autoridades francesas se unen, así, a las belgas, alemanas, españolas y holandesas, que también están investigando el uso de datos por parte de Facebook en un marco de cooperación internacional.

Frente a estas amenazas, lamentablemente confirmadas, la República Francesa ha tomado conciencia del impacto político y técnico de las tecnologías de la información en sus misiones y en la actividad de su administración. Por ello ha formulado diferentes medidas, entre ellas las leyes para prevenir estos sucesos.

La reciente normativa jurídica:

a. La Ley relativa a las medidas de vigilancia de las comunicaciones electrónicas internacionales,[146] conocida como la nueva Ley de inteligencia.[147]

---

[142] "Francia ordena a Microsoft que deje de espiar en Windows 10", [en línea], 30 de julio de 2017, en http://computerhoy.com/noticias/software/francia-ordena-microsoft-que-deje-espiar-windows-10-48456

[143] "Francia da tres meses a Facebook para cumplir con la Ley de Protección de Datos", [en línea], 30 de julio de 2017, en http://www.expansion.com/empresas/tecnologia/2016/02/09/56b9d3c422601d637e8b4649.html

[144] "El Acuerdo de Puerto Seguro con los Estados Unidos de América", [en línea], 30 de julio de 2017, en https://www.agpd.es/portalwebAGPD/internacional/adecuacion/estados_unidos/common/pdfs/ElAcuerdodePuertoSeguroconlosEstadosUnidos.pdf

[145] "Estados Unidos "decepcionado" por el dictamen contra el envió de datos", [en línea], 30 de julio de 2017, en https://elpais.com/internacional/2015/10/06/actualidad/1444154032_422524.html

[146] "Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (1)", [en línea], 15 de marzo de 2018, en https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte

Esta ley tiene como objetivo ampliar la capacidad de vigilancia del servicio secreto. Al permitir medidas de vigilancia para proteger fines generales y poco definidos como los intereses de política exterior, económicos, industriales y científicos de Francia. Además de prevenir la violencia colectiva y la delincuencia organizada con el uso de herramientas de vigilancia masiva que captan llamadas de teléfonos móviles y de cajas negras (con fines antiterroristas) en los proveedores de servicio de Internet que recogen y analizan los datos personales de millones de usuarios de Internet. Geneviève Garrigos, directora de Amnistía Internacional Francia, considera que: "la ley viola flagrantemente los derechos humanos internacionales a la intimidad y a la libertad de expresión".[148]

b. El derecho a la muerte digital:[149]

Permite a todos los individuos organizar en vida las condiciones de conservación y de comunicación de sus datos personales después de fallecer.

c. El derecho al olvido:[150]

En Francia se aplica como la regulación de la red para los menores de edad.

d. Las garantías de acceso y la neutralidad de la red.

Evitan que internet sea un factor de desigualdad social.

e. Derecho a la desconexión.[151]

El pleno ejercicio del trabajador de su derecho a la desconexión y la puesta en marcha por la empresa de dispositivos de regulación de la utilización de los

---

147 "Loi du 24 juillet 2015 relative au renseignement", [en línea], 30 de julio de 2017, en http://www.vie-publique.fr/actualite/panorama/texte-discussion/projet-loi-relatif-au-renseignement.html

148 "Francia: Gobierno vigilará llamadas y datos de internet con nueva ley, denuncia AI", [en línea], 03 mayo de 2017, en http://aristeguinoticias.com/2407/mundo/francia-gobierno-vigilara-llamadas-y-datos-de-internet-con-nueva-ley-denuncia-ai/

149 "¿Cómo gestionar el derecho a la muerte digital?, [en línea], 30 de julio de 2017, en http://www.lavanguardia.com/vida/20160229/4085405270/francia-regula-tratamiento-post-mortem-datos-internet.html

150 "Europa reconoce el derecho al olvido en Internet", [en línea], 30 de julio de 2017, en http://www.lanacion.com.ar/1690239-europa-reconoce-el-derecho-al-olvido-en-internet

151 "Francia reconoce el derecho a desconectar del trabajo", [en línea], 30 de julio de 2017, en https://elpais.com/tecnologia/2017/01/03/actualidad/1483440318_216051.html

dispositivos digitales, a fin de asegurar el respeto del tiempo de descanso y de vacaciones, así como de su vida personal y familiar.

Francia, además, cuenta con una presencia muy relevante dentro de las instituciones internacionales, el Ministerio de Asuntos Exteriores y Desarrollo Internacional vela por la armonización de las posiciones francesas en el extranjero en cuestión de ciberseguridad, como la Unión Europea, la Organización del Tratado del Atlántico Norte (OTAN), la Organización de Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y está contribuyendo activamente a la formulación y el desarrollo de las estrategias futuras en Ciberdefensa.

En contraste, la revista francesa de noticias L'Obs[152] demostró que, en 2015 la Dirección General de Seguridad Externa (DGCE) interceptó y analizó el tráfico de datos internacionales que pasa a través de interceptaciones de cable submarino y el gasto de $775 millones en el proyecto. Información que más tarde confirmaría el jefe técnico de la Dirección General de Seguridad Exterior (DGSE), Bernard Barbier[153] al admitir que durante su gestión (2006 y 2014), realizó un ataque mundial de pirateo informático, mediante un servicio de captación masiva de datos de Internet, equivalente a la NSA estadounidense.

Además, el estado francés mediante la Ley relativa a las medidas de vigilancia de las comunicaciones electrónicas internacionales, ha legalizado el espionaje electrónico a otras naciones, al incorporar, excusar y reafirmar el modelo de NSA estadounidense como una norma global aceptable, comprometiendo los derechos de sus ciudadanos y el de los extranjeros.

Los defensores de los derechos humanos a través de diferentes proyectos; la misión "24 horas antes de 1984",[154] contactaron a los diputados uno por uno

---

[152] "Comment la France écoute (aussi) le monde", [en línea], 15 de marzo de 2018, en https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html

[153] "El espía más indiscreto de Francia", [en línea], 15 de marzo de 2018, en https://elpais.com/internacional/2016/09/03/actualidad/1472893224_106150.html

[154] "Loi renseignement: les écolos décrochent leur télephone pour rallier les députés", [en línea], 01 de agosto de 2018, en http://www.lefigaro.fr/politique/le-scan/2015/05/04/25001-

para tratar de convencerlos de votar contra el proyecto de ley relativa a las medidas de vigilancia de las comunicaciones electrónicas internacionales. El comunicado de La Quadrature du Net, titulado “Shame on France”,[155] el comunicado de prensa conjunto por la Federación Internacional de la Ligas de Derechos Humanos, la Liga de los Derechos Humanos, Reporteros sin Fronteras, Amnistía Internacional, Privacidad Internacional, titulado “Inquiétude des Organisations des Droits de L´homme face á un Projet de Loi Visant á donner aux Agences de Renseignement de nouveaux pouvoirs qui ne sont pas sans danger”,[156] y el informe del Comité Asesor del Consejo de Naciones Unidas para los derechos humanos, advierten que legaliza métodos de vigilancia altamente intrusivos sin garantías de libertad individual y privacidad.

El estado francés como un miembro de la Unión Europea, tiene el compromiso de respetar las normas internacionales de derechos humanos y los principios de protección de datos, es decir, garantizar el derecho a la privacidad de los ciudadanos franceses y extranjeros. Sin embargo, al permitir la vigilancia de las comunicaciones electrónicas internacionales antepone la política exterior, los intereses económicos y científicos de Francia. Quebrantando el derecho a la privacidad y la seguridad nacional de los miembros de la Unión Europea y la del resto del mundo.

2.4 República Federativa de Brasil, líder sudamericano en gobernanza digital

La denuncia por espionaje electrónico del ex técnico de la Agencia de Seguridad Nacional de los Estados Unidos, Edward Snowden, demostró que la República Federativa de Brasil, también era sujeta de esta actividad. Entre los objetivos

---

20150504ARTFIG00184-loi-renseignement-les-ecolos-decrochent-leur-telephone-pour-rallier-les-deputes.php

[155] “Shame on France: French Constitutional Council Widely Approves Surveillance Law”, [en línea], 15 de marzo de 2018, en https://www.laquadrature.net/en/shame-on-france-french-constitutional-council-widely-approves-surveillance-law

[156] “Inquiétude des Organisations des Droits de L´homme face á un Projet de Loi Visant á donner aux Agences de Renseignement de nouveaux pouvoirs qui ne sont pas sans danger”, [en línea], 15 de marzo de 2018, en https://www.ldh-france.org/inquietude-organisations-droits-lhomme-face-projet-loi-visant-donner-aux-agences-renseignement-nouveaux-pouvoirs-pas-danger/

prioritarios de la interceptación de miles de llamadas y correos electrónicos se encontraban personas residentes o en tránsito en Brasil, la ex presidenta *Dilma Rousseff* y la petrolera estatal Petrobras.

Los diarios *The Guardian*[157] y *O Globo*[158] explican que Brasil cuenta con extensas redes digitalizadas públicas y privadas (medios que brindan servicios de comunicaciones a distancia), operadas por corporaciones globales líderes en los sectores de telecomunicaciones, infraestructura de redes, proveedores de internet, sistemas operativos, aplicaciones, entre otros. Lo que convierte a la nación brasileña en un objetivo prioritario en el tráfico de telefonía y datos (origen y destino).

El método que empleo la Agencia de Seguridad Nacional de los Estados Unidos fue: mantener alianzas estratégicas con estas compañías para facilitar el alcance de la red de espionaje electrónico. Un ejemplo fue el programa *Fairview* que utilizó para acceder directamente al sistema brasileño de telecomunicaciones.

La NSA a través de una alianza corporativa con la empresa AT&T[159] de telefonía estadounidense, quien mantenía relaciones de negocios con empresas de telecomunicaciones brasileñas, tuvo acceso a los sistemas de comunicación, y este acceso fue el que permitió a la NSA recoger registros detallados (número de marcado, tronco y extensión utilizados, duración, fecha, ubicación, dirección del remitente y del destinatario, así como direcciones IP y sitios visitados) de llamadas telefónicas y correos electrónicos de millones de personas, empresas e instituciones en Brasil.

El procedimiento se repetía con quien estuviera en la otra punta de la línea o en otra pantalla de computadora. Comienza allí la vigilancia progresiva por la red

---

[157] "The NSA´s mas and indiscriminate spying on Brazilians", [en línea], 02 de agosto de 2017, en https://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying

[158] "EUA espionaram milhões de e-mails e ligações de brasileiros", [en línea], 02 de agosto de 2017, en https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934

[159] "AT&T Helped U.S. Spy on Internet on a Vast Scale", [en línea], 03 de agosto de 2017, en https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html

de relación de cada interlocutor telefónico o destinatario de la correspondencia electrónica (correo electrónico, fax, SMS, vídeos, podcasts, etc.).

Estos hechos encauzaron a Brasil en la búsqueda de alianzas estratégicas (Alemania[160] y Noruega[161]) para reformar las instituciones de gobernanza global responsables de la seguridad en las comunicaciones electrónicas. Una nación a la vanguardia de los derechos digitales, defensora de la privacidad y libertad de expresión en Internet, innovadora de su marco normativo y consciente de su importancia en la comunidad internacional.

En el derecho brasileño, no existe una ley única que garantice el derecho al respeto de la vida privada y familiar, tampoco existe una ley general sobre la protección de datos personales.

Normativa jurídica en Brasil:

a. La Constitución Federal.

En el artículo 5, las secciones X y XII establecen que la privacidad, el honor y la imagen de una persona son derechos fundamentales de cualquier individuo y son inviolables. Además, garantizan el secreto de la correspondencia y de las comunicaciones telegráficas, de datos y telefónicas.

b. El Código Civil.

Establece que la vida privada de un individuo es inviolable.

Aunque no existe una ley única garante del derecho a la privacidad, si existen leyes complementarias como:

- El Estatuto del Niño y la Juventud: protege la imagen y la privacidad de los menores.
- La Ley General de Telecomunicaciones: establece la necesidad de privacidad en el servicio de telecomunicaciones.

---

[160] "Visita del Ministro de Relaciones Exteriores a Alemania – Berlín, 21 de marzo de 2014", [en línea], 06 de agosto de 2017, en http://www.itamaraty.gov.br/es/notas-a-la-prensa/3556-visita-del-ministro-de-relaciones-exteriores-a-alemania-berlin-21-de-marzo-de-2014

[161] "Visita al Brasil del Ministro de Asuntos Exteriores de Noruega, Børge Brende - Río de Janeiro y Brasilia, 19 y 20 de febrero de 2014", [en línea], 06 de agosto de 2017, en http://www.itamaraty.gov.br/es/notas-a-la-prensa/3580-visita-al-brasil-del-ministro-de-asuntos-exteriores-de-noruega-borge-brende-rio-de-janeiro-y-brasilia-19-y-20-de-febrero-de-2014

- El Código Tributario: regula el secreto fiscal.
- La Ley de Secreto Bancario: norma el secreto de las operaciones bancarias.
- El Código de Protección al Consumidor: contiene disposiciones específicas para proteger los datos personales de los usuarios de Internet y los consumidores.
- Ley de la Lista de deudores conformes, en relación con la recopilación, el uso y el intercambio de los datos registrados en las bases de datos de crédito de los contribuyentes que estén en regla.
- Ley de acceso a la información, relativa a los datos personales registrados en bases de datos públicas.

La promulgación del Marco de Derechos Civiles de Brasil para Internet fue parte del esfuerzo para regular los derechos civiles en Internet.

La primera fase del proceso para la construcción de un marco regulatorio de internet en Brasil fue en 2009. La idea se basaba en una propuesta del abogado Ronaldo Lemos realizada en su artículo publicado el 22 de mayo de 2007: "Internet brasileira precisa de um marco regulatório civil".[162] En la segunda fase del proceso se realizó una consulta pública sobre los contenidos de la Ley así como varios foros de discusión durante el 2010.

La tercera fase fue aprobar el Marco Civil de Internet para garantizar los derechos digitales de los ciudadanos y la soberanía tecnológica brasileña. Legislación que entró en vigor el 23 de abril de 2014.

- El Marco Civil de Internet (Marco Civil da Internet) o Ley de Privacidad en Internet,[163] impone límites a los metadatos que pueden ser recolectados de los usuarios de la red en Brasil. También exonera a los proveedores de servicios de Internet de responsabilidad por el

[162] "Artigo: Internet brasileira precisa de regulatório civil", [en línea], 31 de julio de 2017, en https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm
[163] "Lei Nº 12.965, de 23 de abril de 2014", [en línea], 31 de julio de 2017, en http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

contenido publicado por sus usuarios y les exige cumplir las órdenes judiciales para retirar material ofensivo.

El ex ministro de Justicia, José Eduardo Cardozo señaló al respecto: “Creo que la neutralidad, privacidad, libertad y ausencia de discriminación que el texto garantiza realmente va a poner a Brasil a la vanguardia como un modelo para otros países que van a querer... recrear los mismos principios, la misma condición que están consagrados en nuestra ley”.[164]

En el marco de la 34ª reunión del Consejo de Derechos Humanos de las Naciones Unidas (CDH) fue aprobada por consenso la resolución sobre el derecho a la privacidad en la era digital.[165] Un proyecto propiciado por Brasil con apoyo de Alemania, Austria, Liechtenstein, México y Suiza. En la cual se decidió crear la figura de un Relator Especial sobre el Derecho a la Privacidad en la Era Digital, por un periodo inicial de tres años. El Relator deberá presentar un informe anual al Consejo en la 31° sesión (en el 2016) y a la Asamblea General en la 71° (en el 2017/2018), que incluya “observaciones importantes” sobre cómo garantizar este derecho fundamental. El Consejo otorga al Relator Especial la facultad de denunciar las violaciones, “dondequiera que tengan lugar, del derecho a la privacidad” en consonancia con lo establecido en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto de Derechos Civiles y Políticos; y de igual manera “llamar la atención del Consejo y del Alto Comisionado relativo a situaciones de grave inquietud”. Además, el Consejo exhorta la cooperación y asistencia de todos los Estados en el desempeño del mandato del Relator Especial.

Desde entonces, comenzó a investigarse ¿cuáles eran las implicaciones para los derechos humanos?, y si, ¿los gobiernos cuentan con la capacidad tecnológica para llevar a cabo actividades de vigilancia, interpretación y recopilación de datos sobre todas las personas?

---

[164] “Brasil aprueba ley de privacidad en Internet”, [en línea], 31 de julio de 2017, http://www.jornada.unam.mx/ultimas/2014/04/23/congreso-de-brasil-aprueba-ley-de-privacidad-en-internet-4387.html

[165] “El derecho a la privacidad en la era digital”, [en línea], 06 de agosto de 2017, en https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/11/PDF/G1707311.pdf?OpenElement

Sin embargo, existen casos en donde se ha atentado contra el derecho a la privacidad en Brasil:

Entre febrero de 2015 y julio de 2016, cuatro jueces dispusieron el bloqueo temporal en todo el país de la aplicación de WhatsApp, el servicio de mensajería propiedad de Facebook, por no revelar información de sus usuarios relacionada con investigaciones sobre narcotráfico.

En febrero de 2015, un tribunal de Piauí pretendió obligar a WhatsApp para colaborar con el Estado en investigaciones de pedofilia. En diciembre de 2015, un juez del Estado de São Paulo prohibió la aplicación durante 48 horas. En mayo de 2016, un juez de Brasil ordenó el bloqueo de la aplicación de durante 72 horas en todo el país. La jueza *Daniela Barbosa Assunção de Souza*, magistrada de fiscalización de la Sala de Ejecuciones Penales de Río de Janeiro explicó: “la orden judicial no se cumplió a pesar de que esta se reiterara en tres ocasiones". Además, indicó que la empresa muestra un "total desconocimiento de las leyes nacionales" del país en el que opera. "Es la compañía la que ha establecido su filial en Brasil y, por tanto, la que queda sujeta a las leyes y a la lengua nacionales”.[166]

Según la empresa, su política de privacidad garantiza el secreto total de las comunicaciones, ya que están blindados los textos, fotos, videos e incluso las llamadas telefónicas. Únicamente tienen acceso a los contenidos, el emisor y el receptor. "La decisión judicial castiga a más de 100 millones de brasileños que dependen del servicio para comunicarse, administrar negocios y mucho más, para forzarnos a entregar informaciones que afirmamos repetidamente que no tenemos",[167] respondió la empresa en un comunicado.

En marzo de 2016 se presentó otro controvertido caso. Esta vez la policía de *Sao Paulo* arrestó al vicepresidente de *Facebook* para América Latina, *Diego*

[166] “Un juez ordena bloquear WhatsApp en todo el territorio brasileño”, [en línea], 01 de agosto de 2017, en https://elpais.com/internacional/2016/07/19/actualidad/1468941131_714293.html
[167] “La justicia de Brasil bloquea una vez más WhatsApp”, [en línea], 01 de agosto de 2017, en https://elpais.com/tecnologia/2016/05/02/actualidad/1462203263_150504.html

Dzodan, con base en una orden dictada por el juez *Marcel Maia Montalvao*, de Sergipe.

El motivo fue el incumplimiento de WhatsApp (plataforma de mensajería propiedad de Facebook) a una orden judicial que solicitaba acceder a las conversaciones de miembros del narcotráfico de esa ciudad. Ante la negativa de la compañía de proporcionar los datos requeridos, se ordenó el arresto de *Dzodan* por impedir una investigación policial, en el marco de la Ley de Organización Delictiva, que prevé una pena entre tres y ocho años de prisión y una multa a quien impida o, de cualquier forma, dificulte la investigación de una infracción penal que involucre a una organización delictiva.

El presidente del Instituto Brasileño de Derecho Digital, el fiscal *Frederico Ceroy*, sostuvo que el Poder Judicial no estaba solicitando el contenido de los mensajes intercambiados, sino los datos sobre la localización y la identificación de los sospechosos de narcotráfico.

Más aún, los defensores del derecho a la privacidad en internet han expuesto la vigilancia gubernamental de los disidentes. Durante la organización de los eventos deportivos más importantes de la última década, realizados en la nación sudamericana, la Copa Mundial 2014 y los Juegos Olímpicos de Río 2016, los funcionarios del gobierno brasileño gastaron más de 25 millones de dólares en software de recopilación de inteligencia.[168] El espionaje se centró en las amenazas políticas, en la víspera de la final de la Copa del Mundo 2014, la policía de Río arrestó a 19 activistas en sus hogares, después de rastrear sus comunicaciones electrónicas.[169]

En marzo y junio de 2016, fiscales y jueces presentaron más de 40 demandas contra cinco empleados del periódico *Gazeta do Povo* (Gazeta del Pueblo), en el estado de Paraná, en relación con una serie de notas, basadas en

[168] "Brasil aumenta su presupuesto militar para garantizar la seguridad en los Juegos", [en línea], 21 de marzo de 2018, en https://www.infodefensa.com/latam/2016/07/20/noticia-diferentes-agencias-seguridad-brasilenas-defenderan-juegos.html

[169] "Polícia do Rio prende 19 manifestantes na véspera da final da Copa", [en línea], 21 de marzo de 2018, en http://www1.folha.uol.com.br/poder/2014/07/1485042-policia-civil-prende-19-suspeitos-de-vandalismo-no-rio.shtml

información disponible al público en páginas web oficiales, donde se revelaba que jueces y fiscales recibían salarios y beneficios mayores a los permitidos por la Constitución. En julio, la Corte Suprema de Brasil suspendió temporalmente las demandas hasta que ella misma se pronunciara sobre los casos.

En agosto, un juez autorizó a la policía a intervenir el teléfono de un periodista, luego de que éste se negara a revelar quiénes habían sido sus fuentes en una investigación que publicó una lista de ciudadanos brasileños que supuestamente tenían cuentas bancarias en Suiza.[170]

En 2017, la organización de derechos digitales en Brasil, InternetLab presentó su informe titulado "Quem defende seus datos?",[171] evaluación de las políticas de las principales compañías brasileñas de telecomunicaciones, para dictaminar su compromiso con la privacidad del usuario cuando el gobierno solicite los datos personales de sus clientes. El objetivo del informe es alentar a las empresas a competir por los usuarios demostrando quien garantiza su privacidad y protección de datos personales. Este informe forma parte de la iniciativa a nivel continental de los principales grupos de derechos digitales de América del Sur exponiendo las prácticas en materia de privacidad de Internet en la región.

Aunque la República Federativa de Brasil reconoce la privacidad como un derecho fundamental e incluso tiene una conciencia cada vez mayor sobre la vigilancia y la falta de control efectivo de los datos personales. Las actuales leyes complementarias que garantizan la inviolabilidad de la intimidad y la privacidad de los ciudadanos brasileños, son insuficientes para proporcionar seguridad jurídica en el procesamiento de datos personales por parte de entidades públicas y privadas. Existen diferentes reglas para los diversos sectores de la sociedad: financiero, crediticio, salud e Internet. Sin embargo, muchos de estos sectores no pueden, ni deben, tratarse por separado. Por ejemplo, ¿cómo sería posible

[170] "Brasil, eventos de 2016", [en línea], 02 de agosto de 2017, en https://www.hrw.org/es/world-report/2017/country-chapters/298774

[171] "Quem defende seus datos?", [en línea], 20 de marzo de 2018, en http://quemdefendeseusdados.org.br/pt/

separar los servicios financieros y de salud de los servicios prestados a través de Internet?

Es importante mencionar que actualmente el Congreso Nacional analiza el Proyecto de Ley 5.276 / 2016, para resolver esta falta de seguridad jurídica y el Marco Civil de Internet, es un gran paso hacia la implementación del derecho a la privacidad en Internet no sólo en Brasil sino para toda la región.

2.5 República Federal de Alemania, pionera del derecho a la privacidad

Para el pensamiento alemán del siglo XIX, el concepto de libertad era opuesto al determinismo, que se sustenta en la premisa de causa-efecto, es decir, todo acontecimiento físico, incluyendo el pensamiento y acciones humanas (nuestro estado actual) determinan en el algún sentido el futuro. Según recuerda Whitman,[172] en Alemania ser libre no significaba ser libre del control gubernamental o ser libre para implicarse en transacciones bancarias, sino que significaba ejercitar la libre voluntad (autodeterminación) una idea que tiene sus fundamentos en el humanismo.

Entre sus antecedentes del siglo XX, se encuentra la experiencia del régimen nazi, la policía secreta de Hitler, la Gestapo[173] y en la República Democrática Alemana, la Stasi,[174] estos órganos estatales de inteligencia realizaron recolección de datos con fines discriminatorios, supresión y persecución a sus ciudadanos.

Actualmente, Alemania es una nación pionera del derecho a la privacidad. La primera ley de protección de datos (*Datenschutz*) del mundo fue aprobada en

---

[172] "Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital", [en línea], 14 de agosto de 2017, en https://books.google.com.mx/books?id=kRSyCQAAQBAJ&pg=PA96&lpg=PA96&dq=alemania+derecho+a+la+privacidad&source=bl&ots=l9SXIdCtgN&sig=SIyEiZ9WQwqhrj1UJZSAB9uZDtg&hl=es&sa=X&ved=0ahUKEwjgrYrEysbVAhWK7iYKHWp4Aj0Q6AEIXTAJ#v=onepage&q&f=false

[173] "Amigos y enemigos de la Gestapo", [en línea], 10 de agosto de 2017, en http://www.lavanguardia.com/cultura/20160823/404136394894/frank-mcdonough-gestapo-colaboracion-multinacionales-regimen-nazi.html

[174] "Archivos de la Stasi: el rompecabezas más grande del mundo", [en línea], 09 de agosto de 2017, en http://www.bbc.com/mundo/noticias/2012/09/120916_cultura_documentos_archivos_stasi_bd

el estado alemán de *Hessen* en 1970 y la ley federal de protección de datos del país, la *Bundesdatenschutzgesetz*[175] (entre las más estrictas del mundo), fue aprobada en 1977. Estas leyes impiden la transmisión de cualquier dato personal sin la autorización de la persona interesada. La razón de este significativo desarrollo fue su legado histórico.

El derecho a la privacidad y el desempeño de los medios para la población alemana son más que temas de simple debate académico porque han experimentado las consecuencias que supone un Estado con capacidad de una vigilancia masiva. Por ello, la legislación alemana sobre privacidad comienza por aplicar las leyes constitucionales y el derecho general de la personalidad en el momento de regular la privacidad. La ley alemana utiliza el modelo jurídico denominado *Schichtenmodel* o modelo estratificado. El modelo estratificado hace uso de distintas leyes para regular el contenido de las comunicaciones *online*, los servicios prestado *online* y el aspecto técnico.

Normativa jurídica en Alemania:

a. La Constitución de la República Federal de Alemania *(Deutscher Bundestag*).[176] Establece protecciones a la privacidad en:

El artículo 1. Protección de la dignidad humana, vinculación de los poderes públicos a los derechos fundamentales. La dignidad humana es intangible, respetarla y protegerla es obligación de todo poder público. El pueblo alemán, por ello, reconoce los derechos humanos inviolables e inalienables como fundamento de toda comunidad humana, de la paz y de la justicia en el mundo.

El artículo 2. Libertad de acción y de la persona. Toda persona tiene el derecho al libre desarrollo de su personalidad, siempre que no viole los derechos de otros ni atente contra el orden constitucional o la ley moral. Toda persona tiene el derecho a la vida y a la integridad física. La libertad de la persona es inviolable. Estos derechos sólo podrán ser restringidos en virtud de una ley.

---

[175] "Leyes De Protección de Datos Personales en el Mundo y la Protección de Datos Biometricos"- Parte I, [en línea], 09 de agosto de 2017, en https://revista.seguridad.unam.mx/node/2124

[176] "Ley Fundamental de la República Federal de Alemania" [en línea], 15 de agosto de 2017, en https://www.btg-bestellservice.de/pdf/80206000.pdf

El artículo 10. Secreto epistolar, postal y de telecomunicaciones. Son inviolables, las restricciones sólo podrán ser ordenadas en virtud de una ley. Si la restricción está destinada a proteger el régimen fundamental de libertad y democracia o la existencia o seguridad de la Federación o de un Land, la ley podrá disponer que no se informe al afectado y que el recurso jurisdiccional sea reemplazado por el control de órganos y de órganos auxiliares designados por los representantes del pueblo.

El artículo 13. Inviolabilidad del domicilio. Los registros no podrán ser ordenados sino por el juez y, si la demora implicare un peligro inminente, también por los demás órganos previstos por las leyes, y únicamente en la forma estipulada en ellas. Cuando determinados hechos justifican la sospecha que alguien ha cometido un delito particularmente grave y específicamente así predeterminado por la ley, podrán ser utilizados en la persecución del hecho delictivo, con base a una autorización judicial, medios técnicos para la vigilancia acústica de viviendas en las cuales presumiblemente se encuentra el inculpado. Si la investigación de los hechos fuese de otra manera desproporcionadamente difícil o no tuviese ninguna probabilidad de éxito. La medida tiene que ser limitada en el tiempo. En la defensa frente a peligros inminentes para el orden público, especialmente frente a un peligro para la comunidad o para la vida, los medios técnicos para la vigilancia acústica de viviendas sólo podrán ser utilizados con base a una autorización judicial. Una utilización con otra finalidad de los conocimientos recogidos en tal supuesto, sólo será permitida si sirve para la persecución penal o para la prevención ante un peligro y sólo si la legalidad de la medida ha sido verificada previamente por un juez. Por lo demás, las intervenciones y restricciones sólo podrán realizarse para la defensa frente a un peligro común o un peligro mortal para las personas; en virtud de una ley, tales medidas podrán ser tomadas también para prevenir peligros inminentes para la seguridad y el orden públicos, especialmente para subsanar la escasez de viviendas, combatir una amenaza de epidemia o proteger a menores en peligro.

b. La Ley Federal de Protección de Datos (*Bundesdatenschutzgesetz,* (BDSG, in der Fassung vom).[177]

Administra el tratamiento de los datos personales que se procesan en los sistemas de información, comunicación y manualmente. A partir del 25 de mayo de 2018, será reemplazada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en relación con el tratamiento de datos personales y la libre circulación de dichos datos (Reglamento general de protección de datos).[178] Aunque los organismos públicos deberán cumplir tanto con el reglamento como con las leyes de protección de datos de los estados federales alemanes.

La Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983,[179] que declaró inconstitucionales algunos artículos de la Ley del Censo de la República Federal Alemana, ha marcado un hito en la defensa de los derechos de la persona a preservar su vida privada.

c. Ley de Telemedia (*Telemediengesetz*).[180]

Reconocida coloquialmente como: la Ley de Internet, regula el marco legal de los telemedios (servicios electrónicos de información y comunicación; tiendas en línea, casas de subastas en línea, motores de búsqueda, servicios de correo web, podcats, salas de chat, portales web, blogs) en Alemania. Concentra tres leyes diferentes, la Ley de Teleservicios, la Ley de Protección de Datos de Teleservicios y el tratado de los servicios de medios.

d. Ley de Telecomunicaciones (*Telekommunikationsgesetz*).[181]

---

177 "*Bundesdatenschutzgesetz* (BDSG)", [en línea], 14 de agosto de 2017, en http://www.wipo.int/wipolex/es/text.jsp?file_id=328201

178 "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)", [en línea], 23 de marzo de 2018, en https://www.boe.es/doue/2016/119/L00001-00088.pdf

179 "Autodeterminación Informativa", [en línea], 15 de agosto de 2017, en http://www.informatica-juridica.com/trabajos/autodeterminacion-informativa/

180 "*Telemediengesetz*", [en línea], 15 de agosto de 2017, en https://www.lmk-online.de/fileadmin/user_upload/Bilder/01_Die_LMK/06_Rechtsgrundlagen/Telemediengesetz_2016.pdf

Regula la competencia en el campo de las telecomunicaciones. Una de sus contribuciones es la penalización de la interceptación no autorizada de las comunicaciones a través de los canales de telecomunicaciones. Del mismo modo, son penalizados aquellos que poseen, fabrican, distribuyen o importan transmisores inadmisibles (transmisores adecuados para transmitir la palabra hablada sin autorización).

e. La Ley de Aplicación de la Red (*Netzwerkdurchsetzungsgesetz*).

Exige que los operadores de plataformas de Internet (redes sociales)[182] con más de dos millones de usuarios eliminen o bloqueen contenido ilegal en un plazo de 24 horas después de recibir una queja. Además deben informar regularmente sobre su manejo de estas quejas. De lo contrario enfrentan multas de hasta 50 millones de euros.

Es una de las leyes más controvertidas, porque justifica la censura del internet amparada en la lucha contra las noticias falsas, los crímenes de odio, el extremismo derechista o el racismo. Una campaña estatal para legitimar las guerras, la represión, las cazas de brujas, es decir, silenciar a las voces de izquierda y críticas en Internet. El supuesto es que las empresas optarán por eliminar una publicación polémica en lugar de arriesgarse a obtener sanciones financieras severas.

Sin embargo, no existen sanciones contra las plataformas que borren publicaciones legítimas. De este modo, se debilitan los derechos básicos de los usuarios, porque la ley convierte a las grandes corporaciones (Facebook, Twitter, YouTube, etc.) no sólo en fiscales, jueces y jurados, determinando lo que está o no está permitido en Internet. También las autoriza, a proporcionar información sobre los autores de las publicaciones que evoquen quejas.

---

[181] "*Telekommunikationsgesetz*", [en línea], 15 de agosto de 2017, en https://www.gesetze-im-internet.de/bundesrecht/tkg/gesamt.pdf

[182] "El texto de la ley, publicado el 7 de septiembre, define a las redes sociales como proveedores de servicios de telemedios que operan plataformas con fines de lucro en Internet con el fin de permitir que sus usuarios compartan cualquier contenido con otros usuarios o lo pongan a disposición del público."

Normativa jurídica internacional vinculante como estado miembro de la Unión Europea:

- El artículo 8 del Convenio de Europa de Derechos Humanos (CEDH)[183] considera el derecho a la privacidad un derecho fundamental.
- El artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea[184] considera que, toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
- El artículo 12 de la Declaración Universal de Derechos humanos[185] considera que, 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.

La Constitución Alemana de 1949 establece estrictas protecciones de privacidad, no obstante, la jurisprudencia alemana, y en particular las decisiones del Tribunal Constitucional de Alemania (Bundesverfassungsgericht), han reconocido que, el derecho a la autodeterminación de la información es inherente al derecho general de la personalidad, a la luz de las nuevas tecnologías, la información y la comunicación. Por lo tanto, la persona tiene derecho a una protección legal adecuada contra las invasiones a su autodeterminación informativa. Es decir, las leyes que autorizan el monitoreo de la vida privada de presuntos delincuentes en Internet a través de técnicas secretas y remotas de investigación informática han sido declaradas inconstitucionales.

El controvertido caso de los periodistas *Andre Meister* y *Markus Beckedahl*. Después de publicar en su página web Netzpolitik.org[186] documentos confidenciales del gobierno alemán; en los que se detalla como el servicio de

[183] "Convenio Europeo de Derechos Humanos", [en línea], 14 de agosto de 2017, en http://www.echr.coe.int/Documents/Convention_SPA.pdf
[184] "Carta de los Derechos Fundamentales de la Unión Europea", [en línea], 14 de agosto de 2017, en http://www.europarl.europa.eu/charter/pdf/text_es.pdf
[185]"La Declaración Universal de Derechos Humanos", [en línea], 14 de agosto de 2017, en http://www.un.org/es/universal-declaration-human-rights/
[186] "El caso de libertad de expresión que causa conmoción en Alemania", [en línea], 10 de agosto de 2017, en
https://www.bbc.com/mundo/noticias/2015/08/150806_libertad_de_expresion_alemania_lb

inteligencia alemán planeaba crear una unidad especial para monitorear las redes sociales (vigilancia o espionaje *online*), fueron acusados de traición por violación del secreto de Estado.

La reacción fue nacional al denunciar la amenaza contra la libertad de prensa y la violación del artículo 5°[187] de la Constitución Alemana. Y aunque la fiscalía general de Alemania[188] ha cerrado la investigación, surgieron cuestionamientos que es conveniente analizar: ¿Por qué un ministro de Justicia permitió que los periodistas fueran investigados por traición?, ¿previamente las autoridades alemanas habían ordenado la vigilancia de *Meister* y *Beckedahl?*, ¿Cuál era el propósito de vigilar a los periodistas?, ¿qué es un secreto de Estado?, ¿qué le está permitido publicar a un periodista?

La última vez, que el gobierno alemán acuso a un periodista por "alta traición" fue en 1962.[189] No obstante, en pleno siglo XXI, el gobierno alemán ha considerado perjudicial, la denuncia realizada por dos periodistas, en donde exponen documentos clasificados de la vigilancia estatal masiva. Una abierta violación a la libertad de prensa que supuestamente rige en un país, libre y democrático. Los cargos que estuvieron motivados políticamente y visiblemente dirigidos a silenciar, el debate público con respecto a la vigilancia en internet, han costado a los periodistas violaciones a su derecho a la privacidad al ser víctimas de medidas de vigilancia estatal, intimidaciones por no revelar sus fuentes y un posible encarcelamiento, exponiéndolos a sufrir innumerables violaciones a sus derechos humanos.

Una perspectiva más de lo que ofrece la conexión a Internet es la comercialización de productos orientados al mercado infantil. Los riesgos potenciales: recoger los datos personales de menores, como audio e imagen y la

---

[187] "Grundgesetz für die Bundesrepublik Deutschland", [en línea], 12 de agosto de 2017, en https://www.gesetze-im-internet.de/gg/GG.pdf

[188] "Libran cargos por traición periodistas del blog Netzpolitik en Alemania (Video)", [en línea], 12 de agosto de 2017, en http://aristeguinoticias.com/1108/mundo/liberan-cargos-por-traicion-periodistas-de-blog-netzpolitik-en-alemania-video/

[189] De acuerdo al Código Penal alemán, el delito por alta traición contempla la difusión pública de secretos de Estado con la finalidad de perjudicar a Alemania o beneficiar a otro país, y se castiga con uno a cinco años de prisión.

oportunidad delictiva de acceder a los niños sin el permiso ni el conocimiento de sus padres o tutores.

Un caso de protección a los menores lo ejerció el organismo regulador de las telecomunicaciones alemán *(Bundesnetzagentur)*, quien prohibió la venta de "My Friend Cayla",[190] una muñeca interactiva que contiene un micrófono interno, un sistema de reconocimiento de voz con conexión a Internet por tecnología Bluetooth que se controla, a través de una aplicación. Un producto que expone a los menores a diversos peligros, incluyendo el espionaje, la interacción no monitorizada con desconocidos y la explotación comercial de sus conversaciones por parte de la empresa que la fábrica ya que se reserva el derecho a registrar las conversaciones del niño y compartir esa información con terceros.

El presidente de dicho organismo, Jochen Homann, explicaba: "Con un Smartphone y el micrófono, un extraño podría usar la muñeca para escuchar y hablar con el niño sin tener acceso físico al juguete, incluso separado por varias paredes".[191]

Aunque los primeros juguetes de este tipo ya se han retirado del mercado, es conveniente comprobar al adquirir estos productos interactivos: ¿Pueden captar la voz o la imagen de los menores?, ¿dónde se almacena esa información?, revisar la política de privacidad, consultar ¿qué permisos se están concediendo? y ¿a quién? sobre esos datos. Otros países como Francia, Suecia, Grecia, Bélgica, Irlanda y Holanda han comenzado sus investigaciones, esto con el propósito de reforzar la legislación europea en materia de amenazas informáticas.

Entre algunos casos recientes se pueden mencionar los siguientes:

En septiembre de 2016, la aplicación *WhatsApp* propiedad de la empresa estadounidense Facebook modificó su política de privacidad, la cual consiste en:

---

[190] "Prohíben la venta de una muñeca espía en Alemania", [en línea], 09 de agosto de 2017, en http://www.milenio.com/internacional/muena_espia-mi_amiga_cayla-alemania-prohiben_venta-espiar_ninos_0_904709828.html

[191] "Esta muñeca ha sido prohibida en Alemania por espiar a los niños", [en línea], 09 de agosto de 2017, en http://www.eldiario.es/cultura/privacidad/muneca-prohibida-Alemania-espiar-ninos_0_615938787.html

compartir información con otros proveedores de servicio (*Facebook*) y en usar información personal, ya sean datos de uso, cookies, IP, entre otros, con el objetivo de mejorar la calidad del servicio y generar la creación de nuevas características para mejorar la experiencia del usuario. Situación que viola las normativas de seguridad y de privacidad de datos establecidas por Alemania y la Unión Europea.

Son dos empresas independientes que cuentan con datos proporcionados por sus usuarios siguiendo sus respectivos términos de uso y sus políticas de privacidad; sin embargo, la combinación en un mismo dispositivo móvil de *WhatsApp* y *Facebook* deja al usuario completamente desprotegido porque Facebook ni ha solicitado un consentimiento a los usuarios de *WhatsApp*, ni cuenta con una base legal para recibir esos datos.

De acuerdo con la jurisprudencia europea, la red social, que tiene una filial en Hamburgo, debe respetar la legislación alemana de privacidad y transparencia de la información y responder ante los tribunales europeos por las infracciones que sean denunciadas. Sin embargo, Facebook y WhatsApp tienen su matriz en Estados Unidos**,** país en donde las leyes de protección de datos son diferentes que en Europa.

Durante la Primera Cumbre del Consumidor del G20 sobre "Construir un mundo digital en el que los consumidores puedan confiar",[192] fue presentado el estudio internacional elaborado por Consumers Internacional (CI) y la Federación de Organizaciones de Consumidores de Alemania (VZBV), el cual indica que, el 68% de los ciudadanos alemanes están preocupados por la seguridad de sus datos personales en la red.

En Alemania, la privacidad es un derecho civil y la reacción de sus ciudadanos frente al espionaje electrónico (incluida la intervención del teléfono celular de la canciller alemana, Angela Merkel) denunciado por Edward Snowden

[192] "Cumbre del consumidor G20", [en línea], 23 de marzo de 2018, en https://translate.google.com.mx/translate?hl=es-419&sl=en&u=http://unctad.org/en/pages/MeetingDetails.aspx%3Fmeetingid%3D1355&prev=search

fue consecuente y supuso una considerable tensión en las relaciones germano-estadounidenses.

La política alemana respecto a la ley de privacidad, es considerada una de las más estrictas y restrictivas hacia la vigilancia en general, consecuencia de su experiencia histórica. El miedo hacia la recolección de datos se sustenta en un legado de abusos relacionados con la privacidad, la inteligencia y la vigilancia. La terrible experiencia de la Segunda Guerra Mundial cuando los nazis utilizaron la tecnología de IBM para organizar los horrores del Holocausto y el estado de vigilancia de la Stasi, la policía secreta de Alemania Oriental, son datos que se enarbolan cuando se analiza una estrategia preventiva de seguridad nacional, que incluya búsquedas encubiertas de equipos informáticos y retención de datos de telecomunicaciones.

Los atentados en Bruselas[193] y el atentado de Berlín[194] han renovado el debate sobre el secreto de las comunicaciones y sus implicaciones en la seguridad nacional e impulsaron los esfuerzos de las autoridades alemanas para establecer leyes que fortalezcan los poderes de recopilación de inteligencia y la vigilancia estatal en favor de la seguridad nacional.

En particular, los atentados de París y la constatación de que el Estado Islámico recurre a las redes sociales para captar adeptos y comunicarse con sus miembros, actuaron como una llamada de atención para Europa, porque comprendieron que las empresas responsables de la nueva economía de internet, tenían su sede principal fuera del territorio comunitario. Es decir, no servía de nada aplicarles las leyes nacionales para colaborar con la justicia.

Ante estos hechos, los ministros del Interior de Alemania y Francia han solicitado a la Comisión Europea para que obligue a las empresas de internet que gestionan aplicaciones de mensajería móvil (WhatsApp, Telegram, Facebook Messenger, etc.) a proporcionar el contenido de una conversación o permitir el

[193] "Atentado en Bruselas: al menos 30 muertos en el aeropuerto y el metro", [en línea], 23 de marzo, en https://elpais.com/internacional/2016/03/22/actualidad/1458631407_286826.html

[194] "Un hombre mata a 12 personas con un camión en Berlín y reaviva el miedo al terrorismo en Europa", [en línea], 23 de marzo de 2018, en https://elpais.com/internacional/2016/12/19/actualidad/1482176155_449814.html

acceso a la interceptación de las comunicaciones encriptadas. Un planteamiento rechazado por los defensores de los ciberderechos, incluido el supervisor europeo de protección de datos, *Giovanni Buttarelli,* en su último informe.[195] Son los desafíos actuales de seguridad en Europa, que contribuyen a la reconsideración de las posiciones más estrictas sobre la privacidad digital en algunos sectores de la población alemana.

2.6 República de Estonia, líder mundial en gobernanza digital

Estonia es una nación líder en la gobernanza electrónica, los sistemas educativos para las TIC y en la autenticación digital de la identidad. Pionero en el Documento Nacional de Identidad (DNI electrónico), la plataforma X-Road y la firma digital. Referente en la implementación del voto por Internet, ya en 2005, y también del voto por teléfono móvil, en las elecciones de 2008. Desde julio de 2017,[196] cuando asumió la presidencia rotativa de la Unión Europea busca que se reconozca el concepto libre circulación de datos como la quinta libertad del mercado único, junto al libre movimiento de personas, bienes, capitales y servicios. Creador de la primera embajada digital.[197]

El país más desarrollado en términos de avances tecnológicos, su madurez tecnológica supera una década la de otros gobiernos industrializados. Una sociedad electrónicamente exitosa que también encuentra su explicación en la historia.

Después del colapso de la Unión Soviética, Estonia adoptó políticas liberales en términos económicos y sociales. El comunismo dejó la infraestructura en precarias condiciones, un vacío institucional y una pequeña población. Como resultado los gobiernos liberales posteriores concibieron el desarrollo de la

---

[195] "Supervisor Europeo de Protección de datos", [en línea], 24 de marzo de 2018, en https://edps.europa.eu/sites/edp/files/publication/17-05-23_opinion_etias_ex_summ_es.pdf

[196] "La Presidencia del Consejo de la UE", [en línea], 17 de agosto de 2017, en https://www.consilium.europa.eu/es/council-eu/presidency-council-eu/

[197] "Estonia abrirá embajada virtual en Luxemburgo para proteger dato digital", [en línea], 17 de agosto de 2017, en http://www.eluniversal.com/noticias/internacional/estonia-abrira-embajada-virtual-luxemburgo-para-proteger-dato-digital_661502

tecnología de las comunicaciones y la expansión de la información como factores centrales del nuevo modelo de desarrollo. Por lo tanto, el crecimiento de Estonia como estado independiente está ligado a la revolución digital.

Estonia al contar con una economía pequeña fomento la apertura en el comercio y las inversiones. Un progreso que ha llevado al plano internacional mediante una diáspora electrónica sustentada en el interés genuino por el desarrollo digital, sin duda un futuro hábilmente asegurado. El enfoque progresista de Estonia con respecto a la tecnología digital ha tenido beneficios económicos y sociales importantes como los servicios *on-line*, desde administrar las finanzas, registrar las empresas, pagar el estacionamiento o pedir recetas médicas e incluso, votar.

Esta interoperabilidad entre el gobierno y los sistemas de información ha creado paulatinamente un marco normativo para responder a los variables contextos. Un fuerte compromiso político y el respaldo para la digitalización de la administración pública que comenzó en 1990 y que ha continuado con la prioridad de convertir las infraestructuras de información del Estado en un recurso y en la base para la toma de decisiones coherente y la prestación de servicios.

Normativa jurídica en Estonia:

a. El código de identificación personal (*isikukood*).

Desde 1990 se utiliza para identificar de manera singular a cada ciudadano y residente en los sistemas de información del gobierno.

b. El principio de solo una vez.

Desde 1997, la administración pública no puede solicitarle a una persona información que haya proporcionado a cualquier otra oficina estatal.

c. La plataforma oficial de intercambio de datos X-Road.

Desde el 2001 unifica las bases de datos públicas y privadas con los servicios digitales del país. De esta forma, no tiene una puerta de enlace central ni un punto centralizado de gestión. Por lo tanto, la red es más segura porque la información se mantiene en servidores separados.

d. Ley de Firmas Digitales.[198]

Desde 2002 reconoce que las firmas digitales son totalmente equivalentes a las firmas autógrafas, tanto en transacciones comerciales como en transacciones con el sector público. La identificación nacional de Estonia y más tarde la ID-móvil equivalente (en adelante: ID digital nacional) se convirtieron en el elemento esencial de la infraestructura de Clave Personal Nacional (PKI, por sus siglas en inglés), volviéndola un medio legítimo de autenticación y autorización en transacciones digitales, es decir, de firma electrónica.

e. El principio que todo individuo debe tener control sobre cómo se utilizan sus datos personales, y debe poder ver qué servidor público consulta sus datos.

Esto se puso en práctica al crear un mecanismo que registra todo acceso a los datos personales y permite que los individuos utilicen el portal de servicios públicos www.wwsti.ee (o el portal nacional de atención de la salud para los registros de atención medica) a fin de vigilar y ver qué ministerio consultó sus datos. Puede iniciar un procedimiento de reclamación de protección de datos si sospecha que se violó la privacidad.

Además, con el propósito de evitar la compartimentación de responsabilidades ante un incidente cibernético nacional, ha buscado una acción coordinada mediante una estrategia nacional de ciberseguridad desde 2008. Su versión actual (período 2014–17) se centra en garantizar la prestación de servicios vitales, aumentando la capacidad del país para combatir la ciberdelincuencia y mejorar su capacidad de defensa nacional:

- En 2009 se creó el Consejo de Seguridad Cibernética, encargado de apoyar la cooperación entre organismos y supervisar la ejecución de la estrategia, y que depende de la Comisión de Seguridad del Gobierno de la República (un cuerpo ministerial).

[198] "Digitaalallkirja seadus", [en línea], 20 de agosto de 2017, en https://www.riigiteataja.ee/akt/694375

- Además, a la Autoridad del Sistema de Información de Estonia (*Riigi Infosüsteemi Amet*, o RIA) se le concedieron poderes y recursos adicionales para la protección de las redes públicas.
- Se creó el Departamento de Protección de las Infraestructuras Críticas de Información. Responsable de recopilar y almacenar la información crítica de la Infraestructura de la Información (sistemas de información y comunicación, cuyo funcionamiento, confiabilidad y seguridad son importantes para el funcionamiento del Estado).
- En 2011 se creó una Unidad de Defensa Cibernética como parte de la Liga de Defensa de Estonia, una organización voluntaria de defensa interna que lleva su experiencia del sector privado al ámbito público.
- En 2012 se fusionan las unidades de delitos informáticos de la Dirección de la Policía y la Guardia de Fronteras.

Aunado a la protección de las personas, Estonia se ha preocupado por las Leyes en materia de ciberseguridad:

- La Ley de Emergencia de 2009[199]establece que la infraestructura crítica y su aplicación en el sector de las TIC se rige por el Reglamento de Medidas de Seguridad de los Sistemas de Información de Servicios Vitales y Activos de Información Vinculados (2013).[200] Este Reglamento obliga a los proveedores de servicios vitales a notificar los incidentes cibernéticos y presentar informes a la Autoridad del Sistema de Información de Estonia una vez que se restaura la integridad del sistema.
- Ley de Secretos de Estado y de Información Confidencial de Estados Extranjeros de 2007[201] solicita una evaluación anual de la seguridad del

[199] "Hadaolukorra seadus", [en línea], 20 de agosto de 2017, en https://www.riigiteataja.ee/akt/13201475
[200] "Elustahtsa teenuse infosusteemide ning nendega seotoud infovarade turvameetmed", [en línea], 20 de agosto de 2017, en https://www.riigiteataja.ee/akt/120032013007
[201] "Riigisaladuse ja salastatud valisteabe seadus", [en línea], 20 de agosto de 2017, en https://www.riigiteataja.ee/akt/RSVS

almacenamiento digital de documentos gubernamentales clasificados como muy secretos y secretos.

- La Ley de Comunicaciones Electrónicas de 2004 (modificada 2011) autoriza a la Autoridad de Vigilancia Técnica de Estonia a que les solicite a los proveedores de servicios de TIC realizar evaluaciones de la seguridad de sus propios sistemas.
- La Ley de Protección de Datos Personales de 1996 (modificada en 2010)[202] regula el tratamiento de la correspondencia y la información personal. La Ley aplica las normas de protección de datos de la UE, distingue entre datos personales y datos personales sensibles y determina una protección ampliada para los datos personales sensibles.

Después de la serie de ataques cibernéticos iniciados el 27 de abril de 2007, las autoridades de Estonia decidieron realizar una serie de enmiendas al Código Penal estonio para hacer frente a las amenazas cibernéticas.

El espectro de hechos punibles se amplió; la cobertura, la alteración, la eliminación, el daño o el bloqueo de datos ejecutados de manera ilegal; la interferencia u obstaculización del funcionamiento de los sistemas informáticos; la difusión de herramientas maliciosas; la preparación de delitos informáticos y al uso ilegal de los sistemas informáticos, estableciendo en el código penas máximas para las operaciones dirigidas contra servicios o infraestructuras vitales.

Además, otros cambios en el Código Penal han ampliado el alcance de los actos de terrorismo, que incluyen: interferir con datos informáticos o impedir el funcionamiento de los sistemas informáticos, así como amenazar con realizar tales actos, si se cometen con el propósito de obligar al Estado o una organización internacional a una acción u omisión, o interferir de manera grave en la estructura política, constitucional, económica o social del Estado o destruirla, o interferir de manera grave en el funcionamiento de una organización internacional o destruirla, o aterrorizar gravemente a la población.

---

[202] "Isikuandmete kaitse seadus", [en línea], 20 de agosto de 2017, en https://www.riigiteataja.ee/akt/106012016010

Una parte fundamental de la estrategia de Estonia para mejorar su propia seguridad y aumentar su influencia en el exterior es la cooperación con aliados internacionales, medida que fomenta la confianza y reduce los costos. Las organizaciones donde se destaca su participación son: la OTAN, (ejercicios cibernéticos internacionales y foros cibernéticos), la Unión Europea, el Grupo de Expertos Gubernamentales de las Naciones Unidas y la Organización para la Seguridad y la Cooperación en Europa (OSCE).

La infraestructura digital de Estonia es motivo de orgullo nacional, un escenario que seguramente fue considerado para dirigir a esta nación, el primer ataque informativo (ciberataque) contra todo un país en 2007.[203] Su trascendencia reside en la inusitada forma hibrida de utilizar los avances tecnológicos, metodología estudiada por los países y sus academias militares hasta el día de hoy.

El motivo del primer ciberataque a nivel internacional inició con una orden del gobierno de Estonia. La instrucción consistía en trasladar al Soldado de Bronce, que es un monumento en honor a los soldados soviéticos caídos que liberaron a Estonia de los nazis en la Segunda Guerra Mundial; la indicación era llevarlo de Tallin a un cementerio a las afueras de la ciudad. El problema radicó en la divergencia de opiniones; mientras que para los estonios de habla rusa representa la victoria de la Unión Soviética sobre los nazis, para quienes son de etnia estonia, el ejército ruso no fue libertador sino invasor y el Soldado de Bronce es un doloroso recuerdo del medio siglo de ocupación y opresión soviética.

La decisión fue seguida de manifestaciones en las calles debido a noticias falsas en medios rusos que aseguraban que la estatua y las tumbas de militares soviéticos estaban siendo destruidas. El momento más álgido llego el 26 de abril de 2007 en Tallin con dos noches de disturbios y saqueos.

El 27 de abril, Estonia también fue blanco de sucesivos ataques electrónicos que en algunos casos duraron semanas. Las páginas web de bancos,

[203] "Estonia, primera víctima de los 'hackers', [en línea], 20 de agosto de 2017, en https://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html

medios de prensa y organismos gubernamentales colapsaron debido a niveles sin precedente de tráfico en internet. Redes de robots informáticos —conocidos como botnets— enviaron cantidades masivas de mensajes basura (*spam*) y pedidos automáticos online para saturar los servidores. El resultado fue que los estonios se quedaron sin poder usar las webs de casi todos los organismos públicos, y también de bancos locales, periódicos, agencias de noticias.

Todo ello en uno de los países de todo el mundo en que más se utiliza Internet para trámites administrativos y que se ha colocado a la cabeza de los avances en el uso de las nuevas tecnologías para hacer realidad el *open government* y convertirse en una verdadera e-nación.

Los efectos que tuvieron los ciberataques de 2007 en Estonia evidenciaron que estas acciones tienen poco de virtual y que sus consecuencias son del todo reales. Hicieron que se tomara conciencia colectiva sobre las posibles vulnerabilidades a las que se enfrentaban ya que se puede poner en riesgo la seguridad nacional tanto con la paralización de la actividad de las administraciones públicas como de las empresas estratégicas de un país.

La reciente innovación del gobierno estonio contra la ciberguerra es la implantación de una nueva red de embajadas de datos, centros digitales ubicados en terceros países en los que se replicarán las bases de datos fundamentales para que la administración siga funcionando en caso de ataque o catástrofe.

El objetivo es construir una arquitectura de sistemas y datos que se estructure en tres niveles complementarios:

- Primero, tener copias de seguridad de los datos en otro lugar.
- Segundo, contar con esas bases de datos en otro país y que puedan ser utilizadas por el sistema nacional.
- Tercero, tener un sistema completo operativo y constantemente disponible en otro lugar.

"Lo que convierte a las embajadas de datos en algo revolucionario no es su vertiente técnica, puesto que el almacenamiento de información en servidores externos o en la nube es algo que se ha normalizado en los últimos años, sino que

lo realmente novedoso es que sea un gobierno el que implemente esta solución, replicando buena parte de su información, incluida la sensible y clasificada, en diversas localizaciones físicas fuera del territorio nacional",[204] subraya en un reciente informe el grupo de estudio Thiber (The Cybersecurity Think Tank), adscrito al Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid.

Pero ahora que la ciberdefensa es pilar ineludible de las estrategias de seguridad nacional, resulta todo un reto tecnológico y también diplomático en tiempos en que el ciberespionaje se ha demostrado que también puede proceder de los propios países amigos.

El debate mundial se ha centrado en la importancia de la seguridad nacional frente al derecho a la privacidad del individuo.

Los Estados afirman que requieren la concesión, por parte de empresas y ciudadanos, del derecho a la privacidad en el ciberespacio, lo que permitiría el conocimiento y uso de información de las comunicaciones de los ciudadanos para coadyuvar en la lucha contra el crimen organizado y el terrorismo, garantizando así la seguridad pública. Por consiguiente, los gobiernos han realizado prácticas intrusivas como: la vigilancia nacional y extraterritorial, la interceptación de las comunicaciones digitales y la recopilación de datos personales a gran escala. Baste como muestra, el ciberespionaje masivo emprendido por la Agencia de Seguridad Nacional estadounidense.

El cambio de paradigma representado por las nuevas tecnologías que hacen uso de los datos personales, es extremadamente difícil de manejar desde un punto de vista regulatorio. Durante el análisis de las naciones líderes en gobernanza digital, se ha podido constatar que la incorporación de distintos servicios y productos en internet, no han sido totalmente asimilados, incluso por las legislaciones de privacidad más completas.

[204] "¿Por qué Estonia quiere ser líder mundial en ciberdefensa?, [en línea], 20 de agosto de 2017, en http://www.expansion.com/2014/09/09/empresas/tecnologia/1410254908.html

Las actuales políticas de ciberseguridad carecen de un enfoque que salvaguarde los derechos humanos y en particular, el de la privacidad. Desafortunadamente, las principales legislaciones reguladoras de la vigilancia analizadas en este capítulo, no cumplen con las normas internacionales sobre el derecho a la privacidad (eficacia y proporcionalidad). Por el contrario, los gobiernos están manipulando el miedo que sienten sus ciudadanos hacia el terrorismo y el crimen organizado, para aprobar legislaciones intrusivas indebidamente desproporcionadas, que legitiman la vigilancia de las comunicaciones, la interceptación y la recopilación de datos personales en el ciberespacio.

La amenaza progresiva que representa la vigilancia para la privacidad en la era digital. Requiere de la voluntad y la cooperación de los Estados para garantizar la privacidad nacional e internacional como un derecho universal, con rendición de cuentas y salvaguardas sin fronteras, puesto que la vigilancia realizada en el ciberespacio no las tiene.

Sería razonable considerar un nuevo marco de gobernanza para la privacidad y protección de datos, que incluya a miembros de la sociedad civil, representantes gubernamentales, empresas de Internet y expertos en derecho y seguridad para compartir información, conocer sus intereses y poder cubrir todos los aspectos relevantes sobre el adecuado comportamiento estatal en el ciberespacio.

El éxito depende de lograr la sinergia entre los intereses de seguridad y la privacidad en el ciberespacio. Es decir, normas internacionales que permitan a los Estados proteger a sus ciudadanos de las amenazas internas y externas, y que, al mismo tiempo, respeten y velen por sus derechos.

Es comprensible el riesgo que representan las conductas delictivas en el ciberespacio. Por lo tanto, la privacidad y la seguridad son complementarias: en ausencia de seguridad, cualquier intento de proteger los riesgos de privacidad es totalmente inútil. Y la ausencia de privacidad tiende a debilitar la confianza en las

relaciones personales y comerciales, provocando que la seguridad sea un objetivo difícil de alcanzar.

Ante la omisión del principio de complementariedad entre la seguridad y la privacidad en las actuales legislaciones reguladoras de la vigilancia estatal, es imperativo salvaguardar la privacidad en el ciberespacio.

Una de las consecuencias negativas de la vigilancia generalizada, es la transformación del comportamiento de las personas, cuando piensan que están siendo observadas, las disuade de ejercer sus derechos como la libertad de pensamiento y expresión provocando la autocensura. De modo que las personas guardan sus pensamientos para sí mismos o para comunicar furtivamente puntos de vista sólo en persona, un problema para el progreso humano.

Siempre y cuando la toma de decisiones de los involucrados se fundamente en una conciencia de responsabilidad lograremos garantizar la privacidad en el ciberespacio.

Los Estados mediante sus instituciones deben garantizar los derechos que tienen las personas fuera de línea así como en línea, es decir respetar y proteger el derecho a la privacidad también en las comunicaciones digitales. Además de una constante revisión de sus procedimientos, prácticas y legislaciones relacionados con la vigilancia de las comunicaciones, la interceptación y la recopilación de datos personales, comprometidos en la aplicación plena y efectiva de sus obligaciones en virtud del derecho internacional.

Las empresas privadas comprendiendo que, cuanto mayor es el nivel de seguridad ofrecido por las empresas de tecnología, mayor será el grado de confianza en ellas por parte de los usuarios o consumidores, de modo que la competencia mejora y las ganancias incrementan.

Para concluir, los individuos debemos comprender el riesgo que implica interactuar en el ciberespacio y adoptar hábitos seguros. Cada día los usuarios de internet permitimos que las empresas se apoderen de nuestro contenido digital a cambio de servicios gratuitos (correo electrónico, redes sociales, etc.). Sin considerar que nuestros datos personales son parte del nuevo “capitalismo de

vigilancia",[205] en donde la autodeterminación individual es considerada un impedimento para alcanzar los beneficios de la nueva economía. Por lo tanto, se nos despoja de nuestro derecho a la privacidad sin nuestro consentimiento, entendimiento o consentimiento, al guardar información personal y de comportamiento para venderla a los anunciantes que pagan por ella.

¿Por qué es imperativo defender la privacidad? porque al perderla perdemos nuestro poder de decisión, de autonomía y de autoderminación.

[205] "The Wachers: Assaults on privacy in America", [en línea], 29 de marzo de 2018, en https://harvardmagazine.com/2017/01/the-watchers

CAPÍTULO 3. LA IMPORTANCIA DE LAS INSTITUCIONES POLÍTICAS CONTRA EL ESPIONAJE ELECTRONICO EN MÉXICO

Los casos presentados en el capítulo anterior nos permiten reflexionar sobre la importancia que tienen las instituciones públicas, al ser garantes de salvaguardar la soberanía nacional y el orden interno, así como el cumplimiento de las normas constitucionales y legales en amparo y defensa de los derechos de los ciudadanos.

En este tercer capítulo repasaremos los antecedentes de las instituciones que salvaguardan la soberanía nacional en México; constataremos cuáles son los órganos responsables de la seguridad nacional mexicana; comprobaremos el marco jurídico mexicano en materia de seguridad nacional en el que se sustenta la intervención de comunicaciones privadas con el propósito de analizar la actuación de las instituciones responsables de la seguridad nacional, en los casos de espionaje digital, realizados por el gobierno mexicano a periodistas y defensores de derechos humanos en México.

Por último, se contribuirá con una propuesta de políticas públicas para regular el espionaje digital, en donde garantice la rendición de cuentas para la existencia de un Internet libre. En donde la privacidad y la seguridad puedan coexistir en un contexto de Derechos Humanos. Un marco jurídico nacional que regule legítimamente esta actividad desprendida del ejercicio constitucional de la defensa de la soberanía y la garantía de las libertades públicas y privadas. Además de un marco institucional que vele por el cumplimiento de estas normas. Tal vez sea el momento de dejar de ver a la privacidad como un costo de la seguridad, y empezar a verla como un beneficio. Tal vez la privacidad es seguridad y deben ir de la mano una con la otra.

3.1 Antecedentes de las instituciones que salvaguardan la soberanía nacional

Una de las primeras referencias que se hicieron en el marco legal de México sobre seguridad nacional la tenemos en el Código Penal para el Distrito Federal en

Materia de Fuero Común y para toda la República en Materia de Fuero Federal, hoy Código Penal Federal, al establecer en el año de 1970, en su Libro Segundo, Título Primero, los delitos contra la seguridad de la nación, considerando como tales los de traición a la patria, espionaje, sedición, motín, rebelión, terrorismo, sabotaje y conspiración.[206]

Aunque el término seguridad nacional surgió oficialmente en el Reglamento Interior de la Secretaría de Gobernación en 1973,[207] las condiciones políticas, económicas y sociales actuales imperantes en México, distan de aquellas bajo las cuales fue acuñado el término, concebido como una función exclusiva del Estado, debido al tipo de factores que fueron identificados como amenazas a la seguridad nacional, que en su momento se entendía como seguridad del régimen, la protección de sus intereses y su permanencia en el poder. La ausencia de un marco normativo durante muchos años, encubrió un alto grado de discrecionalidad en la estrategia de la defensa de la seguridad nacional y en la toma de decisiones derivadas de esta situación.

Para Piñeyro,

> La falta de acuerdo político y también conceptual sobre qué situaciones sociales pueden ser o no riesgos o amenazas a la seguridad nacional mexicana, es una constante histórica que obedece en gran medida a dos situaciones estructurales. La primera, responde al carácter presidencialista y autoritario del régimen político donde históricamente quien ha definido qué se entiende por seguridad nacional es el presidente en turno y donde los secretarios de Estado durante sus declaraciones públicas sólo repiten el discurso presidencial o plantean generalidades al respecto. La segunda cuestión responde a las múltiples presiones de Estados Unidos para incorporar más a nuestro país a su esquema de seguridad nacional según los intereses, objetivos, retos y peligros de tal esquema y la reticencia de los distintos gobiernos priistas por mantener una variable distancia frente al coloso del norte. [208]

La historia de la seguridad nacional y sus instituciones está ligada a los servicios de inteligencia (civiles y militares) del estado mexicano porque son los

[206] Angulo Jacovo, Juan Manuel, *Op. Cit.*, p. 14.
[207] "Manual de Organización General de la Secretaría de Gobernación", [en línea], 17 de septiembre de 2017, en http://www.diputados.gob.mx/LeyesBiblio/regla/n205.pdf
[208] Angulo Jacovo, Juan Manuel, *Op. Cit.*, p. 4.

encargados de la recolección de información política, militar y económica sobre los otros Estados y particularmente para vencer a los potenciales o reales enemigos del Estado.

El primer antecedente de los servicios de inteligencia en México se remonta a 1918, cuando el presidente Venustiano Carranza creó la Sección Primera de la Secretaría de Gobernación, con la misión de desarrollar actividades de espionaje en el campo enemigo.

Para Bruccet Anaya: “En los años veinte, la responsabilidad gubernamental de perseguir malhechores, y que un porcentaje alto lo hacía organizado, recaía en la llamada Inspección General de la Policía del Distrito, integrada por unos 250 policías. La investigación, fundamentalmente de inteligencia, recaía en las llamadas Comisiones de Seguridad, formadas por un grupo de 50 hombres.”[209]

En 1929, durante el gobierno de Emilio Portes Gil, se creó el Departamento Confidencial, con el propósito de vigilar aliados, enemigos, funcionarios, candidatos y grupos de todo el espectro de la política. Además de vigilar los procesos electorales, visitaba estados y territorios para informar su situación al gobierno central, trasladaba reos federales y deportaba extranjeros indeseables. Contaba con dos clases de agentes: de información política y de policía administrativa.

En 1939, durante el gobierno de Lázaro Cárdenas, se creó la Oficina de Información Política, con el objetivo de realizar investigaciones sobre la situación política del país y prestar los servicios confidenciales que le solicitara el personal de alto nivel de la Secretaría de Gobernación.

Para Bruccet Anaya el 12 de noviembre de 1941, la Jefatura de Comisiones de Seguridad adoptaría la función de servicio secreto.[210]

En 1942, durante el gobierno de Manuel Ávila Camacho, se creó el Departamento de investigación política y social, el cual se encargaba de atender asuntos de orden político interno. Sin embargo, la participación del país en la

[209] Ibídem, p. 219.
[210] Ídem.

Segunda Guerra Mundial hizo necesario ampliar sus funciones con el propósito de cimentar un servicio de inteligencia orientado al control de personas extranjeras.

En 1947, con Miguel Alemán, se creó la Dirección Federal de Seguridad, (DFS) como órgano dependiente de la Presidencia de la República, quedando como encargada de proteger al presidente y a mandatarios que visitaran el país, analizar la información obtenida y realizar operativos espaciales contra los enemigos del régimen.

Dentro de la vida de la DFS es esencial mencionar sus más significativas facetas tales como: la gestión de Don Fernando Gutiérrez Barrios (sin duda el personaje más identificado en la materia), y el papel desempeñado por Javier García Paniagua y Miguel Nazar Haro, también al frente de dicha institución. En este rubro, resulta interesante abordar de manera general algunos de los más significativos acontecimientos, en los cuales se vieron envueltos de manera directa los servicios de inteligencia, por ejemplo, el movimiento estudiantil la faceta insurgente denominada la guerra sucia.

Las tácticas y operaciones de los integrantes del servicio secreto se mantendrían eficazmente funcionando hasta el año de 1967, cuando asumió algunas funciones de la DGIPS y que sería desmantelada en 1985 por sus altos niveles de corrupción, ya que durante la gestión de José Antonio Zorrillo Pérez se llegó al asesinato del periodista Manual Buendía en 1984[211] y del agente de la DEA, Enrique Camarena,[212] así como de su piloto, Alfredo Zavala Avelar en 1985.

En 1985, el presidente Miguel de la Madrid Hurtado creó la Dirección General de Investigación y Seguridad Nacional (DGISEN), con el propósito de establecer un marco funcional y administrativo que integrara mejor las distintas fases de la producción de inteligencia, que permitiera evitar duplicidades entre lo que anteriormente eran la DGIPS y la DFS, y que se eliminaran prácticas que llegaron a comprometer el prestigio y solvencia de esas instituciones. Se hablaba

[211] "El de Buendía, el primer crimen de narcopolítica", [en línea], 29 de octubre de 2017, en http://www.excelsior.com.mx/nacional/2014/05/30/962316

[212] "Kiki Camarena, el caso que México no puede olvidar", [en línea], 29 de octubre de 2017, en https://www.bbc.com/mundo/noticias/2013/08/130821_enrique_kiki_camarena_salazar_caso_dea_narcotrafico_mexico_caro_quintero_an

de rendición de cuentas y de supervisión de operaciones a través del Congreso, de los medios de comunicación y de organizaciones sociales.

En 1989, el presidente Carlos Salinas de Gortari publicó un nuevo Reglamento Interior de la Secretaría de Gobernación, creando el Centro de Investigación y Seguridad Nacional (CISEN) como un órgano administrativo desconcentrado de la citada dependencia, para establecer y operar un sistema de investigación e información para la seguridad del país; recabar y procesar la información generada por el Centro, determinando su tendencia, valor, significado e interpretación específica, para formular conclusiones de las evaluaciones correspondientes; realizando además los estudios de carácter político, económico y social que se relacionen con sus atribuciones.

Los servicios de inteligencia en México, durante el período de 1918 a 1985 se caracterizaron por la práctica generalizada para recopilar la información (espionaje), además de la falta de análisis de la misma para producir una adecuada inteligencia. Desde su fundación la falta de institucionalización y la distorsionada relación con el sistema político llevaba a que los servicios de inteligencia se involucraran en las disputas por el poder, influyendo en el proceso de toma de decisiones, desempeñando funciones de una policía política que se distinguió por la violación de las garantías individuales y por su corrupción.

Lo anterior se comprende, desde una perspectiva de largo plazo, derivado del limbo jurídico y político en el que se hallaban, sin duda indispensable para que funcionaran con discrecionalidad e impulsaran agendas personales. El corolario fue la malinterpretación del concepto de seguridad nacional, cuándo se presentaron las verdaderas amenazas a la seguridad nacional, estas fueron sobredimensionadas y se erró el método usado en su eliminación, tal fue el caso del movimiento estudiantil y del periodo denominado la guerra sucia.

3.2 Evaluación de las instituciones que salvaguardan la soberanía nacional

De acuerdo al Artículo 89 de la Constitución Política de los Estados Unidos Mexicanos (vigente) entre las facultades y obligaciones del Presidente se

encuentra: preservar la seguridad nacional, en los términos de la ley respectiva, y disponer de la totalidad de la Fuerza Armada permanente o sea del Ejército, de la Armada y de la Fuerza Aérea para la seguridad interior y defensa exterior de la Federación.[213]

En la conducción de tal política, el titular del Poder Ejecutivo se orienta por principios normativos como son: los principios generales de política exterior, la autodeterminación de los pueblos; la no intervención; la solución pacífica de controversias; la proscripción de la amenaza o el uso de la fuerza en las relaciones internacionales; la igualdad jurídica de los Estados; la cooperación internacional para el desarrollo; el respeto, la protección y promoción de los derechos humanos; y la lucha por la paz y la seguridad internacionales; en la doctrina de defensa, basada en los planes DNI, DNII y DNIII, y corresponde al primero la defensa ante un enemigo externo, el segundo al mantenimiento del orden interno, y el tercer al despliegue militar para la protección de la población en casos de desastre; en el diseño de políticas gubernamentales que logren el desarrollo socioeconómico del país; y la gobernabilidad bajo un sistema democrático de gobierno, que garantice la convivencia pacífica entre los mexicanos.

Para fines administrativos la responsabilidad de garantizar la seguridad nacional, la soberanía, las instituciones públicas, así como para ejercer vigilancia y protección de la integridad, los límites territoriales y los límites marítimos del estado mexicano, recae en tres principales secretarias de Estado.

La Secretaría de la Defensa Nacional[214] (el Ejército y la Fuerza Aérea), la Secretaria de Marina[215] (la Armada), es decir, las Fuerzas Armadas, mediante las

---

[213] "Constitución Política de los Estados Unidos Mexicanos", [en línea], 18 de septiembre de 2017, en http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf

[214] "Manual de Organización General de la Secretaría de la Defensa Nacional", [en línea], 10 de octubre de 2017, en https://www.gob.mx/cms/uploads/attachment/file/48566/M.O.F._Secretar_a_de_la_Defensa_Nacional.pdf

[215] "Manual General de Organización de la Secretaría de Marina", [en línea], 11 de octubre de 2017, en https://www.gob.mx/cms/uploads/attachment/file/200287/MANUAL_GENERAL_DE_ORGANIZACION_DE_LA_SEMAR.pdf

Secciones Segundas del Estado Mayor generan inteligencia militar para la seguridad nacional.

La Secretaría de Gobernación mediante el Centro de Investigación y Seguridad Nacional (CISEN), un organismo descentralizado de la citada institución, con autonomía técnica, operativa y de gasto, adscrito directamente al Titular de dicha Secretaría. Su función es generar inteligencia civil en materia económica, social y política para la toma de decisiones de alto nivel en materia de seguridad nacional, cuyas atribuciones son:

- Operar tareas de inteligencia como parte del sistema de seguridad nacional,
- Recabar y procesar la información,
- Preparar estudios de carácter político, económico, social y demás que se relacionen con sus atribuciones,
- Elaborar los lineamientos generales del plan estratégico y la Agenda Nacional de Riesgos,
- Establecer la coordinación y cooperación interinstitucional con las diversas dependencias de la Administración Pública Federal,
- Adquirir, administrar y desarrollar tecnología especializada para la investigación y difusión confiable de las comunidades del Gobierno Federal en materia de Seguridad Nacional, así como para la protección de esas comunicaciones y de la información que posea, además de prestar auxilio técnico a cualquiera de las instancias representadas en el Consejo.

Aunque existen dependencias y unidades administrativas que ostentan el reconocimiento como Instancias de Seguridad Nacional: la Secretaría de Comunicaciones y Transportes por medio de la Dirección General de Aeronáutica Civil; la Secretaría de Hacienda y Crédito Público a partir de la Dirección General de Inteligencia Financiera; la Secretaría de Seguridad Pública mediante la Policía Federal; la Procuraduría General de la República, a partir del Centro Nacional de Planeación y Análisis de la Información para el Combate a la Delincuencia

(Cenapi) y la Agencia Ministerial de Investigación; la Secretaría de la Función Pública a partir de la Dirección General de Información e Integración y la Secretaría de Relaciones Exteriores.

En 2005, durante la administración del ex presidente Vicente Fox Quesada, se publicó el decreto por el que se expide la Ley de Seguridad Nacional en la que se considera la existencia de un Consejo de Seguridad Nacional, una instancia deliberativa, con la finalidad de establecer y articular la política de seguridad nacional, y se atribuye funciones que lo hacen ser el órgano máximo en la materia, quedando a cargo del presidente de la República la toma de decisiones, por ser el responsable de garantizar la seguridad nacional del Estado Mexicano.

Integrado por el titular del Ejecutivo Federal, quien lo presidirá; el secretario de Gobernación, quien fungirá como secretario ejecutivo; el secretario de la Defensa Nacional; el secretario de Marina; el secretario de Seguridad Pública; el secretario de Hacienda y Crédito Público; el secretario de la Función Pública; el secretario de Relaciones Exteriores; el secretario de Comunicaciones y Transportes; el procurador general de la República, y el director general del Centro de Investigación y Seguridad Nacional. Además, el Consejo cuenta con un secretario técnico, que es nombrado por el presidente de la República, de quien dependerá en forma directa, y cuenta con un equipo técnico especializado y recursos asignados en el Presupuesto de Egresos de la Federación. Sin embargo, la ley dispone que éste no formará parte del Consejo.

Por tanto, conocerá los asuntos siguientes:

- La integración y coordinación de los esfuerzos orientados a preservar la seguridad nacional;
- Los lineamientos que permitan el establecimiento de políticas generales para la seguridad nacional;
- El Programa para la Seguridad Nacional (2014-2018)[216] y la definición anual de la Agenda Nacional de Riesgos;

[216] "Programa para la Seguridad Nacional 2014-2018", [en línea], 09 de octubre de 2017, en http://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014

- La evaluación periódica de los resultados del Programa para la Seguridad Nacional y el seguimiento de la Agenda Nacional de Riesgos;
- Los programas de cooperación internacional;
- Las medidas necesarias para la SN, dentro del marco de atribuciones previsto en la Ley de Seguridad Nacional y en otros ordenamientos aplicables;
- Los lineamientos para regular el uso de aparatos útiles en la intervención de comunicaciones privadas;
- Los lineamientos para que el CISEN preste auxilio y colaboración en materia de Seguridad Pública, procuración de justicia y en cualquier otro ramo de la Administración Pública que acuerde el Consejo;
- Los procesos de clasificación y desclasificación de información en materia de Seguridad Nacional, y
- Los demás que establezcan otras disposiciones o el presidente de la República.

Algunas de las atribuciones que la Ley de Seguridad Nacional no les otorga a las instancias responsables de esta asignatura, se establecen en Reglamento para la coordinación de acciones ejecutivas en materia de seguridad nacional.[217]

En la Ley de Seguridad Nacional también se estipula que las políticas y acciones vinculadas con la seguridad nacional estarán sujetas al control y evaluación del Legislativo Federal por conducto de una comisión bicameral integrada por tres diputados y tres senadores. La presidencia de la Comisión será rotativa y recaerá alternadamente en un senador y un diputado. La cual contará con las siguientes atribuciones:

- Conocer el proyecto anual de la Agenda de Seguridad Nacional y emitir una opinión.
- En los meses en que inicien los periodos ordinarios de sesiones del Congreso, el Secretario Técnico del Consejo, deberá remitir a la citada

[217] "Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional", [en línea], 09 de octubre de 2017, en http://www.diputados.gob.mx/LeyesBiblio/regla/n18.pdf

comisión un informe general de las actividades desarrolladas en el semestre inmediato anterior.

- Solicitar copia de los informes de actividades que en envié el Director General del CISEN al Secretario de Técnico.
- Solicitar copia de los informes generales de cumplimiento de las directrices que de por escrito el Secretario Ejecutivo al Director General del CISEN.
- Requerir información respecto a los acuerdos de cooperación que establezca el CISEN y las acciones instrumentadas para tal efecto.
- Requerir al CISEN y a las instancias correspondientes los resultados de las revisiones, auditorias y procedimientos que se practiquen a dicha institución.
- Enviar al Consejo cualquier recomendación que considere apropiada.

La presente Ley dispone que la seguridad nacional se rija por principios de legalidad, responsabilidad, respeto a los derechos fundamentales de protección a la persona humana y garantías individuales y sociales, confidencialidad, lealtad, transparencia, eficiencia, coordinación y cooperación.

Establece que, ninguna persona estará obligada a proporcionar información a los servidores adscritos al Centro de Investigación y Seguridad Nacional (CISEN), y que los datos personales de los sujetos que proporcionen información serán confidenciales, sin que se pueda en ningún caso divulgar información reservada, que a pesar de no tener vinculación con amenazas a la seguridad nacional o de acciones o procedimientos preventivos de las mismas, lesionen la privacidad, la dignidad de las personas o revelen datos personales.

Sin embargo, como toda legislación, es perfectible y, por tanto, deja espacios a la reflexión y critica sobre la seguridad nacional.

Del contenido de la ley se argumenta que la seguridad nacional tiene un notable enfoque penal, al establecer como amenazas a la seguridad nacional conductas que pueden ser tipificadas como delitos en la mayoría de los supuestos, sin considerar los desastres naturales, la falta y contaminación del agua, la

pobreza, los daños de la ecología, la inmigración, entre otros, que también pueden constituir en un momento dado serias amenazas a la seguridad nacional.

Por ejemplo, el listado de amenazas a la seguridad nacional dejó algunas ambigüedades como: los actos contra la seguridad de la aviación, el personal diplomático y la navegación marítima. En donde la acción de un pasajero alcoholizado en el interior de un avión o un ladrón que ingresa a la embajada podrían catalogarse bajo una perspectiva amplia como una amenaza a la seguridad nacional.

De igual modo, las amenazas más precisas como: actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada, denotan confusión, pues estas son situaciones reales o amenazas. Es decir, la ley contiene algunas amenazas que de hecho son riesgos, los que requieren acciones prospectivas y preventivas que eviten la conformación de una amenaza, de cara a la cual predominan las acciones disuasivas y operativas.

Esta confusión queda plasmada cuando se menciona la obligación de elaborar la Agenda Nacional de Riesgos basada en el Plan Nacional de Desarrollo del gobierno en turno. Es decir, la Ley consiente que el gobierno en turno incluya las amenazas que considere convenientes, porque no existe una agenda concreta sino un listado de amenazas cambiantes; por ejemplo, el sida para algunos países africanos es una amenaza a la seguridad nacional o el narcotráfico para ciertas republicas latinoamericanas, pero mientras estén bajo control estatal serán un riesgo.

Para Jorge Chabat, la Ley de Seguridad Nacional se debería llamar: Ley que Reglamenta la Actividad de Inteligencia del CISEN, porque establece los casos en que el servicio de inteligencia civil (CISEN) puede hacer inteligencia y básicamente intervenir comunicaciones para espiar ciudadanos comunes y corrientes.

Actualmente, existen tratados y acuerdos internacionales celebrados por México en materia de seguridad nacional.

- Acta final de la Segunda Conferencia Internacional de la Paz o Segunda Conferencia de La Haya.[218] Establece la mejora de las normas que rigen el arbitraje, la guerra, la neutralidad y el Convenio de Ginebra.
- Convención Interamericana sobre Personalidad y Capacidad de Personas Jurídicas en el Derecho Internacional Privado.[219] Define la "persona jurídica" como una entidad con existencia y personalidad propia. Así mismo, específica que la Ley aplicada será la del lugar en donde se constituyó. Finalmente, establece que la Ley declarada aplicable podrá no ser aplicada en el territorio del Estado que la considere manifiestamente contraria a su orden público.
- Acuerdo entre los Estados Unidos Mexicanos y la República de Guatemala sobre Cooperación para Combatir el Narcotráfico y la Farmacodependencia.[220] Por medio de este acuerdo se crea el Comité Guatemala-México de Cooperación para Combatir el Narcotráfico.
- Tratado de Cooperación Mutua entre el gobierno de los Estados Unidos Mexicanos y el gobierno de la República de Guatemala, para el Intercambio de Información respecto de Operaciones Financieras Realizadas a través de Instituciones Financieras para Prevenir, Detectar y Combatir Operaciones de Procedencia ilícita o de Lavado de Dinero.[221] Permite y facilita, de manera recíproca, el intercambio de información sobre operaciones financieras entre las Partes, a fin de detectar y asegurar operaciones financieras (colocación, ocultación, cambio o transferencia de activos) que se sospeche se realizaron con

[218] "Acta final de la Segunda Conferencia Internacional de la Paz", [en línea], 02 de agosto de 2018, en https://archivos.juridicas.unam.mx/www/bjv/libros/3/1158/6.pdf
[219] "Decreto por el que se aprueba la Convención Interamericana sobre Personalidad y Capacidad de Personas Jurídicas en el Derecho Internacional Privado.", [en línea], 27 de septiembre de 2017, en http://www.dof.gob.mx/nota_detalle.php?codigo=4638093&fecha=06/02/1987
[220] "Decreto Promulgatorio del Acuerdo entre los Estados Unidos Mexicanos y la República de Guatemala sobre Cooperación para Combatir el Narcotráfico y la Farmacodependencia", [en línea], 27 de septiembre de 2017, en http://dof.gob.mx/nota_detalle.php?codigo=4653865&fecha=04/03/1992&print=true
[221] "Decreto Promulgatorio del Tratado de Cooperación Mutua entre el Gobierno de los Estados Unidos Mexicanos y el Gobierno de la República de Guatemala para el Intercambio de Información respecto de Operaciones Financieras", [en línea], 27 de septiembre de 2017, en http://www.dof.gob.mx/nota_detalle.php?codigo=698258&fecha=05/03/2003

recursos provenientes de actividades ilícitas. Además, se establecen los mecanismos y acciones a cargo de las Partes.

- Convención de Viena sobre Relaciones Diplomáticas (1961),[222] tiene como finalidad el mantenimiento de la paz, la seguridad internacional, privilegios e inmunidades diplomáticos para el desarrollo de las relaciones amistosas entre las naciones, prescindiendo de sus diferencias de régimen constitucional y social.
- Tratado Interamericano de Asistencia Recíproca (TIAR) o Tratado de Río. Fomenta la seguridad colectiva en el Hemisferio, al definir las medidas y procedimientos que gobiernan la respuesta colectiva de los Estados parte, bajo la consideración de que cuando un Estado miembro sufra un ataque armado, éste debe ser considerado un ataque a todos. Además plantea las medidas para responder a las agresiones que no se consideran ataques armados.
- Tratado Americano de Soluciones Pacíficas o Pacto de Bogotá.[223] Se reafirman los compromisos contraídos por anteriores convenciones y declaraciones internacionales, así como por la Carta de las Naciones Unidas, se convino en abstenerse de la amenaza, del uso de la fuerza o de cualquier otro medio de coacción para el arreglo de controversias y en recurrir en todo tiempo a procedimientos pacíficos, previamente a la posibilidad de llevarlas al Consejo de Seguridad de la ONU.

Ante la creciente inseguridad originada por el terrorismo y la delincuencia organizada y por ser una prioridad para la gran mayoría de los estados, la seguridad nacional es una de las fuentes principales para la celebración de tratados, acuerdos y alianzas entre los países. Además, al interior de los Estados se le ha otorgado mayor importancia al fortalecimiento de las instituciones encargadas de desarrollar estos temas.

---

[222] "Convención de Viena sobre Relaciones Diplomáticas", [en línea], 27 de septiembre de 2017, en http://www.cndh.org.mx/ DocTR/2016/JUR/A70/01/JUR-20170331-II14.pdf

[223] "Tratado Americano de Soluciones Pacíficas", [en línea], 27 de septiembre de 201, en http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-42_soluciones_pacificas_pacto_bogota.asp

Por consiguiente, es primordial una reflexión sobre la eficacia de la normatividad internacional, no sólo por ser instrumentos del orden jurídico nacional con el carácter de norma suprema; sino también, por ser el medio por el que los Estados y las organizaciones internacionales adquieren derechos y obligaciones como sujetos de Derecho Internacional. Son el instrumento jurídico que contiene y constata de manera fehaciente la voluntad de las naciones para cooperar en la solución de los problemas comunes de la humanidad, estrechar las relaciones de amistad entre los pueblos y coexistir pacíficamente en un ambiente de voluntad política y buena fe en el cumplimiento de los compromisos adquiridos.

No obstante, la falta de poder coercitivo o entidades supranacionales que garanticen el cumplimento de las normas entre sujetos de derecho jurídicamente iguales, aunado a las diferentes necesidades e intereses de cada Estado originan dificultades para lograr una cooperación y coordinación en cuanto a políticas y estrategias, por lo que, la adopción de instrumentos jurídicos internacionales relativos a incrementar la seguridad internacional es complejo.

Desde los atentados del 11 de Septiembre, las agendas de seguridad nacional se han orientado a la defensa. Es decir, hacia el uso de la fuerza para defender, asegurar y garantizar el bienestar de su población.

La concepción de una sociedad internacional consciente de respetar las decisiones e intereses de cada Estado, buscando el apoyo mutuo para obtener mayores beneficios a un bajo costo es una creencia lejana a nuestra realidad, porque al momento de definir cada país sus necesidades, se tiende a caer en las subordinaciones de unos con otros, sin tomar en cuenta que cada uno de los intereses y estrategias es tan válido como las otras.

3.3 Casos de Espionaje en México

El 24 de agosto de 2016, los investigadores del Citizen Lab de la Universidad de Toronto documentaron el método de infección del malware Pegasus,[224] desarrollado por la empresa israelí NSO Group.[225] En términos generales, la infección consiste en el envío de un mensaje SMS al usuario con un texto que busca engañarlo, mediante el uso de *técnicas de ingeniería social*,[226] para hacer clic en un enlace adjunto. Al hacer clic en el enlace, el navegador se abre y redirige al usuario a uno de los sitios web de la infraestructura de NSO Group, dándole la oportunidad al malware de instalarse en el dispositivo gracias a una vulnerabilidad en el sistema operativo. De este modo, el atacante gana acceso a los archivos guardados en el equipo, así como a los contactos, mensajes y correos electrónicos. Además de obtener permisos para usar, sin que el usuario lo sepa, el micrófono y la cámara del dispositivo.

En el informe "Gobierno espía, vigilancia sistemática a periodistas y defensores de derechos humanos en México"[227] realizado por Red en Defensa de los Derechos Digitales, Article 19 y SocialTIC, se reveló que México era el país al que está dedicada la mayor parte de la infraestructura de NSO Group. Al exponer una serie de ciberataques realizados entre enero de 2015 y julio de 2016, mediante el malware Pegasus, en contra de periodistas y defensores de derechos humanos en México, con la intención de espiar sus comunicaciones, después de acciones públicas y críticas contra el gobierno mexicano.

---

[224] "Pegasus: el software espía definitivo para iOS y Android", [en línea], 08 de octubre de 2017, en http://www.eluniversal.com.mx/articulo/techbit/2017/04/20/pegasus-el-software-espia-definitivo-para-ios-y-android

[225] "NSO Group: Los espías israelíes que hackean iPhone con un solo SMS", [en línea], 02 de agosto de 2018, en https://www.forbes.com.mx/nso-group-los-espias-israelies-que-hackean-iphones-con-un-solo-sms/

[226] "Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas", [en línea], 02 de agosto de 2018, en https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

[227] "Gobierno espía, vigilancia sistemática a periodistas y defensores de derechos humanos en México", [en línea], 09 de octubre de 2017, en https://r3d.mx/gobiernoespia/.

El informe detalla que los objetivos fueron:

1. *Los Miembros del Centro de Derechos Humanos Miguel Agustín Pro Juárez, A.C. (Centro Prodh)*: Entre abril y junio de 2016, Mario Patrón (director del Centro Prodh), Stephanie Brower (coordinadora del área internacional del Centro Prodh) y Santiago Aguirre (subdirector del Centro Prodh) recibieron mensajes de textos con intentos de infección de Pegasus, durante la investigación y defensa de casos en donde existían violaciones a los derechos humanos como: los cuarenta y tres normalistas de Ayotzinapa, la ejecución de veintidós civiles en el municipio de Tlatlaya (Estado de México),[228] las sobrevivientes de tortura sexual durante el operativo de San Salvador Atenco en 2006[229] y la discusión de la Ley General contra la Tortura.[230]
2. *Miembros del equipo de investigación de Aristegui Noticias:* Desde enero de 2015 hasta julio de 2016, Carmen Aristegui**,** Rafael Cabrera, Sebastián Barragán y el hijo de la periodista Emilio Aristegui **—**menor de edad en el momento de recibir los intentos de infección vinculados a la infraestructura de Pegasus—, están relacionados con fechas posteriores a la divulgación de investigaciones de Aristegui Noticias, como: el reportaje sobre empresarios del Estado de México beneficiados con las licitaciones sin competencia,[231] las denuncias de tortura dentro de la Procuraduría General de Justicia del Estado de México,[232] la

[228] "Posibilidad de ejecución en Tlatlaya: ONU", [en línea], 18 de octubre de 2017, en http://archivo.eluniversal.com.mx/primera-plana/2014/impreso/posibilidad-de-ejecucion-en-tlatlaya-onu-47032.html

[229] "Me quitaron la mitad de mi vida: el dolor de la mujeres de Atenco, diez años después", [en línea], 18 de octubre de 2017, en https://www.nytimes.com/es/2016/09/22/me-quitaron-la-mitad-de-mi-vida-el-dolor-de-las-mujeres-de-atenco-diez-anos-despues/

[230] "Informe de seguimiento del Relator Especial sobre la tortura y otros tratos o penas crueles, inhumanos o degradantes-México",[en línea], 18 de octubre de 2017, en http://www.hchr.org.mx/images/doc_pub/InformeSeguimientoRelatorONUTortura2017.pdf

[231] "Licitaciones a modo benefician a empresarios cercanos a Peña Nieto", [en línea], 24 de octubre de 2017, en http://aristeguinoticias.com/0905/mexico/licitaciones-a-modo-benefician-a-empresarios-cercanos-a-pena-nieto/

[232] "Frente Mexiquense acusa a PGJEM: tortura, fabrica delitos y capertas de investigación", [en línea], 11 de octubre de 2017, en https://www.proceso.com.mx/439688/frente-mexiquense-acusa-a-pgjem-tortura-fabricar-delitos-carpetas-investigacion

investigación de los Panama Papers,[233] el enfrentamiento en Nochixtlán,[234] lo que sugiere una relación con su trabajo.

3. *Carlos Loret de Mola*: entre agosto y septiembre de 2016 recibió nueve mensajes (intentos de infección con el Pegasus). La coyuntura eran las denuncias realizadas por el periodista sobre los hechos ocurridos en Tanhuato, Michoacán,[235] el caso del exgobernador Javier Duarte,[236] la crisis de derechos humanos en el país[237] y la Ley General del Sistema Nacional Anticorrupción por parte del PRI en el Senado.[238] De Mola aclaró que: "El espionaje no es un asunto menor",[239] porque los métodos utilizados por los perpetradores de estos ataque demuestran que el país goza de impunidad para aquellos que desean amedrentar a los periodistas, además de quererlos hacer sentir vulnerables y quererlos hacer que saben sobre sus investigaciones.
4. *Miembros del Instituto Mexicano para la Competitividad, A.C. (IMCO):* en diciembre de 2015, el Director General, Juan Pardinas, recibió mensajes de texto vinculados a Pegasus, durante la preparación para presentar la iniciativa de la #Ley3de3.[240] En mayo de 2016, la Directora de Educación e Innovación Cívica, Alexandra Zapata, recibió los

---

[233] "*Panama Papers*: Criminales, políticos y los negocios turbios que esconden sus fortunas", [en línea], 24 de octubre de 2017, en http://aristeguinoticias.com/tag/panama-papers/

[234] "Hechos en Nochixtlan dejan 6 muertos y 21 detenidos", [en línea], 24 de octubre de 2017, en http://www.eluniversal.com.mx/articulo/estados/2016/06/19/hechos-en-nochixtlan-dejan-6-muertos-y-21-detenidos

[235] "Tanhuato: la barbarie y la impunidad", [en línea], 19 de octubre de 2017, en http://www.jornada.unam.mx/2016/08/29/opinion/018a1pol

[236] "Javier Duarte", [en línea], 19 de octubre de 2017, en http://aristeguinoticias.com/tag/javier-duarte/

[237] "La crisis de derechos humanos que nos alcanzó", [en línea], 19 de octubre de 2017, en http://www.proceso.com.mx/466497/la-crisis-derechos-humanos-nos-alcanzo

[238] "Aprueba Senado Ley General del Sistema Nacional Anticorrupción", [en línea], 19 de octubre de 2017, en http://comunicacion.senado.gob.mx/index.php/informacion/boletines/29206-aprueba-senado-ley-general-del-sistema-nacional-anticorrupcion.html

[239] "El espionaje no es un asunto menor: Carlos Loret de Mola (Video)", [en línea], 19 de octubre de 2017, en http://aristeguinoticias.com/1906/mexico/el-espionaje-no-es-un-asunto-menor-carlos-loret-de-mola-video/

[240] "Entran ciudadanos a debatir Ley 3 de 3", [en línea], 23 de octubre de 2017, en https://www.reforma.com/aplicacioneslibre/articulo/default.aspx?id=812139&md5=5da1733bc52731710eec3e373d947d99&ta=0dfdbac11765226904c16cb9ad1b2efe&lcmd5=ac9e7b9ce8e96066b5ed38c876dc33e4

ciberataques cuando el Congreso acordó un periodo extraordinario para discutir leyes anticorrupción incluyendo #Ley3de3.

5. *Miembros de Mexicanos contra la Corrupción y la Impunidad (MCCI):* Entre mayo y junio de 2016, Salvador Camarena, director general de investigación periodística, y, Daniel Lizárraga, jefe de información de la unidad, fueron atacados con el software Pegasus, los mensajes coinciden con las publicaciones hechas por estos periodistas tras la difusión de sus investigaciones: "La Casa Blanca",[241] "El caso de las empresas fantasma de Veracruz"[242] y el caso de David Korenfeld[243].

El caso más preocupante de espionaje electrónico en México, por las implicaciones que tendría en el derecho internacional, son los *ciberataques perpetrados en contra del Grupo Interdisciplinario de Expertos Independientes (GIEI)*, que gozaban de privilegios e inmunidades reconocidos en la Convención de Viena sobre Relaciones Diplomáticas, para investigar un caso que se ha vuelto paradigmático de la situación de los derechos humanos en México.

La desaparición de los 43 estudiantes normalistas de Ayotzinapa, el 26 de septiembre de 2014, tras enfrentamientos con la policía y cuyos cuerpos fueron presuntamente incinerados, aunado a una versión oficial del gobierno mexicano que nunca dejó claro el motivo: provocaron la exigencia del pueblo mexicano de una investigación independiente con el objetivo de esclarecer los eventos y con la esperanza de encontrar a los jóvenes.

El gobierno aceptó el escrutinio internacional y la Comisión Interamericana de Derechos Humanos (CIDH) nombró a un grupo de cinco expertos: abogados destacados y activistas del mundo hispanohablante para indagar el caso.

En pocos meses la relación entre el GIEI y las autoridades se deterioró. La presión del gobierno era cada vez mayor, los miembros del grupo realizaron

---

[241] "La casa blanca de Enrique Peña Nieto (investigación especial)", [en línea], 23 de octubre de 2017, en http://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/

[242] "El caso de las empresas fantasma de Veracruz", [en línea], 23 de octubre de 2017, en http://www.animalpolitico.com/2016/12/desaparece-el-gobierno-de-veracruz-645-millones-de-pesos-entrega-el-dinero-a-empresas-fantasma/

[243] "Renuncia David Korenfels como director de Conagua", [en línea], 24 de octubre de 2017, en http://www.excelsior.com.mx/nacional/2015/04/10/1017862

acusaciones públicas indicando la interferencia y obstaculización de las autoridades mexicanas en sus indagatorias como: el rechazo a compartir documentos o permitir la realización de entrevistas clave e, incluso, con una indagatoria penal en represalia a su trabajo. En su informe final rechazaron la versión oficial del gobierno sobre lo sucedido a los estudiantes desaparecidos, al mencionar que no había evidencia de un incendio suficientemente poderoso como para haber incinerado 43 cuerpos y que ningún hueso o fragmento entre los restos coincidían con los de los desaparecidos.

El espionaje forma parte de lo que los investigadores calificaron como una campaña de acoso e interferencia a sus indagatorias. De acuerdo con la evidencia forense, el teléfono celular del secretario ejecutivo (jefe de misión), principal enlace del Grupo Interdisciplinario de Expertos Independientes (GIEI), el 1 de marzo y el 4 de marzo de 2016, recibió mensajes de texto con un hipervínculo que escondía el programa Pegasus. Ese teléfono celular del secretario ejecutivo del grupo fue utilizado por la mayoría de los integrantes del GIEI, al fungir como un nexo de comunicación entre los investigadores, sus fuentes, la CIDH y el gobierno de México.

Los investigadores enviaron una carta privada al secretario ejecutivo de la Comisión Interamericana de Derechos Humanos a finales de junio en el que detallaban sus sospechas sobre los intentos de vigilancia a los periodistas y defensores de derechos. Además del teléfono, dijeron que otros dos celulares recibieron mensajes sospechosos.

“Si esto le puede suceder a un órgano independiente que tiene inmunidad y que fue invitado por el mismo gobierno, da miedo pensar qué le podría pasar a un ciudadano común en México”,[244] añadió Francisco Cox, abogado chileno e integrante del GIEI.

[244] “Investigadores del GIEI dicen que fueron espiado para entorpecer la investigación del caso Ayotzinapa”, [en línea], 25 de octubre de 2017, en https://www.nytimes.com/es/2017/07/10/pegasus-giei-espionaje-ayotzinapa/

Aunque “no hay prueba alguna de que agencias del Gobierno mexicano sean responsables del espionaje”,[245] debido a que el software Pegasus no deja rastros del hacker que lo utilizó.

En el caso mexicano se ha documentado su adquisición por al menos tres dependencias de gobierno en México: la Secretaría de la Defensa Nacional (SEDENA), la Procuraduría General de la República (PGR, Fiscalía)[246] y el Centro de Investigación y Seguridad Nacional (CISEN).

En julio de 2012 salieron a la luz ocho contratos secretos de la Secretaría de Defensa Nacional a través de los cuales ésta había adquirido un complejo sistema de espionaje (incluía el programa Pegasus, de NSO) por “5 mil 628 millones de pesos”[247] a la empresa Security Tracking Devices, S.A de C.V, con sede en Jalisco, propiedad de José Susumo Azano Mansura. Algunos de los cuales estaban bajo investigación de la Auditoría Superior de la Federación y la Contraloría de las Fuerzas Armadas.

En enero de 2014, una filtración de correos de la empresa italiana Hacking Team,[248] reveló que los empleados del CISEN ya conocían el programa de infección de teléfonos móviles y los habían probado con diferentes sistemas operativos como Android, BlackBerry, iOS.

Entre 2014 y 2015, durante la administración de Jesús Murillo Karam, la PGR compró el software de espionaje Pegasus por “15 millones de dólares”[249].

En 2016, activistas digitales preguntaron oficialmente a la Fiscalía qué servicios había adquirido de NSO Group. La respuesta oficial fue ambigua. “La

---

[245] “No hay pruebas de espionaje por parte del gobierno: Presidencia”, [en línea], 25 de octubre de 2017, en http://www.eluniversal.com.mx/articulo/nacion/politica/2017/06/19/no-hay-pruebas-de-espionaje-por-parte-del-gobierno-presidencia

[246] “Pegasus tuvo al menos seis responsables en PGR, entre 2014 y 2016”, [en línea], 09 de octubre de 2017, en http://aristeguinoticias.com/0307/mexico/pegasus-tuvo-seis-responsables-en-pgr-entre-octubre-de-2014-y-2016/

[247] “Paga Sedena 5 mmdp por equipo para espiar”, [en línea], 25 de octubre de 2017, en http://archivo.eluniversal.com.mx/notas/859221.html

[248] “Una filtración revela el uso de hackers por el Gobierno mexicano”, [en línea], 25 de octubre de 2017, en https://elpais.com/internacional/2015/07/07/actualidad/1436220111_034556.html

[249] “Pagó gobierno de México 15 millones de dólares a firma de ciberespionaje: NYT”, [en línea], 25 de octubre de 2017, en http://aristeguinoticias.com/0309/mexico/pago-gobierno-de-mexico-15-millones-de-dolares-a-firma-de-ciberespionaje-nyt/

Agencia de Investigación Criminal (un área de la PGR localizó la información solicitada… la misma constituye información clasificada como reservada"[250]), fue la respuesta de la PGR.

De acuerdo con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental,[251] por información reservada se entiende aquella que puede comprometer: la seguridad nacional, la seguridad pública, la defensa nacional, la conducción de las negociones internacionales, la estabilidad financiera, económica o monetaria del país, la vida, la seguridad o la salud de cualquier persona, o causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado.

La información reservada por razones de seguridad nacional es, cuando la difusión de la información ponga en riesgo acciones destinadas a proteger la integridad, estabilidad y permanencia del Estado Mexicano, es decir, implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipos útiles a la generación de inteligencia para la Seguridad Nacional.

No podrá invocarse el carácter de reservado cuando se trate de la investigación de violaciones graves de derechos fundamentales o delitos de lesa humanidad. La información reservada, podrá ser desclasificada cuando se extingan las causas que le dieron origen o cuando haya transcurrido el periodo de reserva (hasta por doce años), protegiendo la información confidencial (información personal de los gobernados) que en ella se contenga. Aunque sí la información es extemporánea puede transformar un dato útil o necesario en uno

[250] "El Gobierno mexicano declaró secretos los contratos sobre el software del espionaje a periodistas", [en línea], 25 de octubre de 2017, en https://elpais.com/internacional/2017/06/20/mexico/1497984473_017962.html
[251] "Ley Federal de Transparencia y Acceso a la Información Pública", [en línea], 27 de octubre de 2017, en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf

completamente carente de valor. La disponibilidad de esta información será sin perjuicio de lo que, al respecto, establezcan otras leyes.

Otro aspecto controversial de la información reservada es la clasificación porque las autoridades u órganos encargados de llevarla a cabo, necesariamente deben apegarse a la normatividad y lineamientos establecidos para ello; sin embargo, también depende de la aplicación de otros ordenamientos jurídicos secundarios, según la materia e institución de que se trate. De igual manera, depende en muchos casos de la interpretación que le de cada sujeto encargado.

Más aún, ¿cómo podemos confiar los ciudadanos mexicanos, en que nuestro gobierno sea capaz de investigarse a sí mismo?

Sí, el sistema institucional responsable de brindar certidumbre es cuestionado a causa de la vigilancia digital perpetrada por algunas dependencias de gobierno en México. De donde se infiere que, la participación libre y segura de la sociedad civil es acotada por un sistema de control que ha dejado en estado de indefensión a los ciudadanos, vulnerando su derecho a la privacidad, sin que medie una orden judicial.

Es importante recordar que uno de los propósitos de los ciberataques es inspirar pánico y conseguir un acceso rápido a los teléfonos celulares, hechos que despiertan cuestionamientos legales y éticos sobre el abuso por parte del gobierno –o elementos rebeldes en su interior– de tecnología cibernética altamente sofisticada y costosa.

Conforme al artículo 16 de Constitución Política de los Estados Unidos Mexicanos, en su noveno párrafo, las comunicaciones privadas son inviolables, y la ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas. Además, el mismo párrafo dispone que exclusivamente la autoridad judicial federal, a petición debidamente fundada y motivada 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, salvo que se trate de las materias de carácter electoral,

fiscal, mercantil, civil, laboral o administrativos, o en el caso de las comunicaciones del detenido con su defensor.

Acorde con lo anterior, la Ley de Seguridad Nacional, en sus artículos 34 y 35, establece que de conformidad con lo dispuesto en el párrafo noveno del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el Centro de Inteligencia y Seguridad Nacional deberá solicitar en los términos y supuestos previstos por dicha ley, autorización judicial para efectuar intervenciones de comunicaciones privadas en materia de seguridad nacional, entendiendo por intervención de comunicaciones la toma, escucha, monitoreo, grabación o registro que hace una instancia autorizada, de comunicaciones privadas de cualquier tipo y por cualquier medio, aparato o tecnología.

La solicitud de intervención de comunicaciones privadas sólo procederá cuando se esté en uno de los supuestos que se establecen en el artículo 5 de la misma ley, considerados como amenazas a la seguridad nacional por el legislador federal, entre las que se encuentran los actos tendientes a consumar espionaje, sabotaje, terrorismo, subversión, traición a la patria, genocidio en contra de los Estados Unidos Mexicanos dentro de territorio nacional, actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado mexicano, actos que impidan a las autoridades actuar contra la delincuencia organizada, actos tendientes a quebrantar la unidad de las partes integrantes de la Federación, actos tendientes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada, actos contra la seguridad de la aviación, entre otras, que por su naturaleza atentan en forma inmediata y directa contra la estabilidad y permanencia del Estado nacional, siendo éste el único caso en que se pueda autorizar al Centro de Intervención de Comunicaciones Privadas.

Las demás instancias de la seguridad nacional no tienen permitido por la ley intervenir las comunicaciones. Por disposición de la propia ley, la autorización de intervención de comunicaciones privadas tendrá sólo una vigencia temporal por un lapso no mayor a 180 días naturales, y en casos de excepción debidamente

justificados, el juez podrá autorizar prórroga a dicho plazo, hasta por un periodo igual al de la autorización original.

El artículo 61 de la ley invocada obliga a los servidores públicos cuyas áreas estén relacionadas con la seguridad nacional, a orientar, con base en los principios previstos en el artículo 3°de la misma, el desempeño de sus funciones, preservando los de legalidad, responsabilidad, respecto a los derechos fundamentales y garantías individuales y sociales, confidencialidad, lealtad, transparencia, eficiencia, coordinación y cooperación, que deben cumplir en términos de las disposiciones legales que regulan el servicio público.

La ley de la materia expresamente limita la función de las autoridades, al disponer en su artículo 62 que fuera de los casos y condiciones previstos en la misma, ninguna persona estará obligada a proporcionar información a los servidores adscritos al CISEN, es decir, prohíbe que los responsables de la seguridad nacional puedan obtener de manera forzosa alguna información relacionada con la seguridad nacional, en contra de la voluntad de los ciudadanos.

En materia de procuración de justicia, la Ley de Seguridad Nacional dispone en su artículo 25 que el Centro será auxiliar del Ministerio Público de la Federación y prestará cooperación, apoyo técnico y tecnológico, intercambio de información sobre la delincuencia organizada y las demás acciones que se acuerden por el Consejo, observando en todo momento respecto a las formalidades legales, las garantías individuales y los derechos humanos, lo cual viene a constituir una limitación más a las funciones de las instancias de seguridad nacional, al obligarlas a respectar en todo momento las garantías individuales y los derechos humanos en su actuación.

Otra limitación que la ley de la materia impone a las instancias responsables de la seguridad nacional la encontramos en el artículo 31, al ejercer atribuciones propias en la producción de inteligencia, las instancias gozarán de autonomía técnica y podrán hacer uso de cualquier método de recolección de información, pero ello será sin afectar en ningún caso las garantías individuales ni los derechos humanos.

Con lo anterior, el legislador federal garantiza que las funciones desarrolladas por los órganos responsables de generar inteligencia para la seguridad nacional no incurran, en aras de preservar esta asignatura, en la comisión de conductas que vulneren o restrinjan las garantías individuales ni los derechos humanos de la población.

Otros cuestionamientos, están relacionados con las empresas desarrolladoras de este tipo de software, que en su mayoría operan al amparo de las lagunas legales: ¿Las empresas pueden realmente controlar el uso de herramientas de vigilancia masiva, armas cibernéticas, etc.? ¿Por qué, son las empresas las que deciden hasta qué punto profundizan en la vida personal de los ciudadanos? Y ¿Cuál es el papel de Estado? ¿Cuáles son las sanciones para las empresas que los comercializan? ¿Existen controles de importación y exportación de estos sistemas?

"NSO Group dijo que: vendió Pegasus sólo a gobiernos, únicamente después de revisar sus prácticas en materia de derechos humanos y exclusivamente tras establecer como condición que se usara para vigilar a criminales y terroristas. Sin embargo NSO reconoció que, después de la venta, no tiene control sobre cómo se usa el programa espía".[252]

El ciberespionaje es un tema que cobra relevancia cuando constatamos sus efectos. En particular, cuando es el gobierno quien lo realiza en contra de ciudadanos nacionales o extranjeros.

El marco normativo que regula la intervención de comunicaciones privadas en México son:

1. La Constitución de los Estados Unidos Mexicanos (art.16)
2. El Código Penal Federal (artículos 177 y 211 Bis)
3. La Ley de la Policía Federal (art. 48)
4. La Ley Federal contra la Delincuencia Organizada (art. 11 bis 1)

[252] "Editorial: Cuando los gobiernos no se resisten a abusar de los programas espía", [en línea], 27 de octubre de 2018, en https://www.nytimes.com/es/2017/07/11/editorial-programas-espia-mexico-pegasus-gobiernoespia/

5. El Código Nacional de Procedimientos Penales (art. 252)
6. La Ley de Seguridad Nacional (art. 33)

Intervenir las comunicaciones de los particulares (toma, escucha, monitoreo, grabación o registro por cualquier medio, aparato o tecnología) sin una autorización judicial es una violación al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. En otras palabras, cualquier acto que atente contra la libertad y privacía de las mismas será sancionado por la Ley.

En contraste con lo anterior, el derecho a la privacidad se ve limitado por el mismo artículo cuando menciona que: solamente 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.

Es importante reiterar que es una facultad limitada y existen diversos requisitos que las instituciones dependientes del Poder Ejecutivo deben cumplir para obtener la autorización de un juez y posteriormente acceder a las comunicaciones privadas de una persona.

- En el caso de la Procuraduría General de la República (PGR), y las fiscalías de las 32 entidades federativas, el Código Nacional de Procedimientos Penales (CNPP) en los artículos 292 a 302 contempla la intervención de comunicaciones privadas cuando se requiere investigar un delito.
- Por lo que se refiere a la Policía Federal, Ley de la Policía Federal en su artículo 48, autoriza las intervenciones cuando se constate la existencia de indicios suficientes sobre la organización o ejecución de un delito.
- En cuanto al Centro de Investigación y Seguridad Nacional (CISEN) la intervención de comunicaciones privadas sólo se puede solicitar cuando existe una amenaza inminente a la seguridad nacional.

Conforme a la normativa anterior, sin la autorización del Poder Judicial de la Federación ninguna otra instancia gubernamental en México puede autorizar este tipo de intervenciones.

El delito de intervención ilegal a las comunicaciones privadas es considerado grave por el Código Penal Federal (CPF), en los artículos 177 y 211 Bis, se contemplan penas de seis a doce años de prisión para cada uno de los implicados. Además, se prevé que los imputados o acusados por dicho delito tengan que pagar multas que van de los 300 a 600 días del salario mínimo vigente.

El derecho a la privacidad igualmente está incluido en la legislación mexicana por medio de los tratados internacionales de los que México es parte:

- La Declaración Universal de los Derechos Humanos (artículo 12).
- La Convención Americana sobre Derechos Humanos (art. 11).
- El Pacto Internacional de Derechos Civiles y Políticos (artículo 17).

Si bien la normatividad existente contempla el derecho a la vida privada. Las actuales tesis emitidas por la Suprema Corte de Justicia de la Nación (SCJN), indican que no es un derecho absoluto y que se puede restringir en la medida en que las injerencias no sean abusivas o arbitrarias.

En caso de que, la determinación de la denuncia presentada ante la Procuraduría General de la República (PGR) por el delito de espionaje gubernamental fuera a favor de los activistas y periodistas como toda la evidencia sugiere. Se acreditaría la comisión de diversos delitos como: violación de correspondencia, acceso ilícito a sistemas y equipos de informática. No obstante, el delito de espionaje considera únicamente el robo de información confidencial por parte de mexicanos o extranjeros para ser vendida a gobiernos de terceros países. En otras palabras, el espionaje se define de manera tradicional, por lo que no se contempla el espionaje gubernamental y sólo se castiga la intervención ilegal de comunicaciones privadas, electrónicas o en papel, así como el acceso ilícito a equipos informáticos, categoría que incluye computadoras y teléfonos inteligentes.

Por otro lado, aunque la legislación mexicana considera el delito de espionaje, la institución encargada de investigar el ilícito depende de quién sería el presunto responsable de esa invasión a la privacidad personal.

Algunos especialistas defienden la existencia de una regulación de los delitos informáticos en la legislación penal mexicana y que basta con analizarla para adecuarla de forma pormenorizada al uso de la tecnología. Es decir, adecuar y procesar un ciberdelito respecto de la norma vigente; pero es innegable la necesidad de una reforma legislativa para incluir un catálogo de delitos informáticos que regule el ciberespionaje para que la tecnología siga creciendo sin perjuicio de los usuarios y de la sociedad.

3.4 Propuesta de políticas públicas

Una de las preocupaciones centrales de los diversos sectores de la sociedad mexicana es la vigencia y el fortalecimiento del Estado Derecho, cuyo propósito es crear y asegurar las condiciones de existencia, que satisfagan las necesidades del grupo de individuos que le dieron origen y posibilitar la vida ordenada en sociedad.

Aunque históricamente el Estado mexicano se ha mantenido a la vanguardia en su sistema legislativo, específicamente en los rubros de promoción, defensa y garantía de los derechos humanos, tanto en el plano nacional como en el contexto internacional.

A través de la adopción los sistemas de protección:

1. El sistema jurisdiccional que establece el orden jurídico nacional para dirimir las controversias que se den por violación o en aplicación de la ley, entre ellas las que protegen los derechos humanos de las personas.
2. El sistema no jurisdiccional de protección de los derechos humanos, se materializa por medio de la institución de origen sueco llamada ombudsman, conocida en otros países como “defensor del pueblo” o “procurador de derechos humanos”.

No obstante, su aplicación efectiva aún no se ha logrado, sin duda, existen normas jurídicas que protegen las garantías fundamentales de las personas, pero su simple declaración no es suficiente. Se requieren cambios legislativos que constituyan la base para promover una nueva práctica en el ejercicio del poder, debido a la impartición de justicia y especialmente las violaciones ocurridas durante el proceso penal.

Por lo que se refiera a los derechos humanos en el ciberespacio, considerados la cuarta generación de derechos humanos (la universalización del acceso a la tecnología, la libertad de expresión en la Red y la libre distribución de la información), las tecnologías de la información y la comunicación, también están transformando nuestra concepción y aplicación de los mismos. Baste, como muestra que actualmente crear y reeducar consumidores, así como, colonizar conciencias a través de valores implícitos en los productos audiovisuales se incluyen en las definiciones de invasión y esclavitud.

Por otra parte, el capítulo anterior de esta investigación, nos permitió observar los mecanismos de dominación, ataque y violación de los derechos humanos en el ciberespacio. En donde, la limitación del acceso a las condiciones necesarias (técnicas, económicas o culturales) evitan el desarrollo de formas más avanzadas de participación pública como el intercambio y la libre expresión de las creencias e ideas.

Del mismo modo, constatamos que la creencia generalizada sobre la aparente inmaterialidad e invisibilidad de los delitos en el ciberespacio es errónea, cuando los flujos de información mediante cables y satélites traspasan las fronteras que creíamos barreras impermeables, disminuyendo nuestras libertades, estándares de vida, provocando un desequilibrio entre el poder personal e institucional, que nos aleja cada día de una sociedad democrática.

Por lo tanto, el estado mexicano requiere un constante desarrollo para garantizar los derechos humanos en ciberespacio, mediante un análisis multidisciplinario y creativo que aporte soluciones políticas coherentes, en donde, se reconozcan las nuevas necesidades humanas para aprovechar dichos medios,

y los nuevos derechos que son inherentes al hecho mismo del vivir en una sociedad tecnológica.

Así mismo, un marco jurídico nacional y el establecimiento de mecanismos y procedimientos orientados a garantizar los derechos humanos en el ciberespacio. Para brindar certeza a la sociedad mexicana que las instancias de procuración de justicia, cuentan con las herramientas necesarias (códigos penales, leyes complementarias) para investigar los ciberdelitos y sancionar a los ciberdeliencuentes con apego a derecho.

El marco institucional es otro tema central, porque brinda y vela por el cumplimiento de las normas. En el caso mexicano, es necesario redimensionar el concepto de seguridad nacional, ya que, no corresponde íntegramente al mundo globalizado en el que hoy vivimos. El sobredimensionamiento de los riegos y las amenazas a la seguridad nacional, han provocado un deficiente aprovechamiento de las habilidades institucionales con una planeación estratégica inadecuada; una cooperación internacional limitada y una excesiva rigidez en la estructura de mando.

Como resultado, la imagen pública del Estado es altamente cuestionada por algunos sectores de la sociedad, quienes consideran que las amenazas más apremiantes a la seguridad nacional provienen del Estado mismo. Sin duda, una problemática alarmante, porque se cuestiona la existencia misma del Estado al no contar con instituciones fuertes que gobiernen de manera eficiente, es decir, que no cumplen con su razón de ser.

Los Estados pueden tomar las medidas necesarias para proteger su seguridad, sin embargo, no pueden ejercer el poder sin límite alguno o valerse de cualquier procedimiento para alcanzar sus objetivos, a causa de que, ninguna actividad de éste puede fundarse sobre el deprecio a la dignidad humana. El ejercicio de la función pública tiene unos límites claramente establecidos que derivan precisamente del hecho de que los derechos humanos son atributos de la dignidad humana y, por lo tanto, superiores al poder del Estado.

No obstante, existen Estados que controlan y limitan el libre flujo de información a través de Internet, coartando las libertades fundamentales de sus ciudadanos, justificando sus acciones en los perjuicios de internet como: la transmisión de valores propios de sociedades decadentes, los cuales, representan una amenaza para la soberanía nacional y transgreden las costumbres y tradiciones nacionales. Rusia y su Estrategia para el Desarrollo de la Sociedad de la Información para 2017-2030, ilustran esta información.

Por otra parte, algunos Estados se percataron que sus ciudadanos utilizan internet, como un foro público, en donde, tienen una mayor capacidad de organización horizontal y cuestionan los valores establecidos por los actores sociales que han monopolizado el acceso a los medios de comunicación. Por lo tanto, actúan en consecuencia para mantener su influencia social mediante campañas de sensibilización social sobre una serie de conductas delictivas realizadas a través de internet –pornografía infantil, propaganda racista, apología del terrorismo y violencia, etc.– con el propósito de legitimar la censura y la catalogación de los contenidos de las páginas Web en supuesta defensa de los valores morales. Francia y la Ley relativa a las medidas de vigilancia de las comunicaciones electrónicas internacionales, ilustran la información.

A su vez, el estado mexicano ha buscado enmarcar los delitos electrónicos, en figuras típicas como robo, fraude, falsificación, daños, estafa, sabotaje, entre otros. Basándose en la premisa de que éstos se tratan de meras variaciones de otros delitos ya existentes fuera del ámbito del Internet.

Sin embargo, existen transgresiones totalmente nuevas, la seguridad nacional de todo el globo se ve amenazada por el ciberterrorismo. El debate mundial sobre la gobernanza en internet es consecuencia de los constantes ciberataques. La responsabilidad de los intermediarios en internet sobre la ciberseguridad, y el ciberespionaje, tema de esta tesis, son conductas que requieren una respuesta clara de todos los sujetos involucrados e interesados para instrumentar políticas que construyan un ciberespacio más seguro.

Definitivamente la regulación de los ciberdelitos implica una gran labor considerando las innumerables lagunas y ambigüedades que pueden surgir al revisar cada caso o situación. Así mismo, se tiene plena conciencia de las dificultades que enfrentan las naciones para desarrollar marcos jurídicos que regulen el ciberespionaje como son: el anonimato en internet, el desarrollo exponencial de la tecnología, la reducción de costos y tiempo, la correcta aplicación de medidas de seguridad y la ingeniería social.

El reto para México, además de comprender la amenaza que representa el ciberespionaje es la modificación o armonización de su marco jurídico en materia de ciberdelitos. Sirva de ejemplo, el delito de espionaje, considerado aún de forma tradicional en la legislación mexicana, es decir, sólo se contempla el robo de información confidencial por parte de mexicanos o extranjeros para ser vendida a gobiernos de terceros países. Una definición poco consecuente con las necesidades de la sociedad de la información y por lo tanto, no permite afrontar íntegramente los riesgos y amenazas en materia de ciberseguridad.

Las instancias de procuración de justicia requieren ser dotadas de herramientas jurídicas para la persecución del ciberespionaje y sancionar no sólo a los funcionarios encargados de la inteligencia (la Ley de Seguridad Nacional se concentra en regular las actividades del CISEN), sino también a los legisladores y a cualquier otro funcionario que, en favor de o en interés de la seguridad nacional, realicen actividades de vigilancia estatal (ciberespionaje gubernamental), violando el derecho a la privacidad de los individuos.

A su vez, la Estrategia Nacional de Ciberseguridad será un desafío más, que enfrentará la próxima administración, puesto que, transformar a México en una nación que aprovecha con responsabilidad el potencial de las TIC y es resiliente ante los riesgos y amenazas en el ciberespacio requiere transitar de la estrategia a la acción.

Con el propósito de contribuir a uno de los objetivos de la Estrategia Nacional de Ciberseguridad mexicana, titulado sociedad y derechos, el cual, busca generar las condiciones para que la población realice sus actividades de manera

responsable, libre y confiable en el ciberespacio. Y, ante la existencia de legislaciones internacionales, en donde, se contemplan derechos digitales como: Derecho a la muerte digital, el Derecho al olvido y el Derecho a la desconexión.

Se ha tomado como referente a la República Federal de Alemania, una nación pionera del derecho a la privacidad, así como, del ejercicio de la libre voluntad (autodeterminación), fundamentos del humanismo, para proponer la creación de un organismo independiente, que sea un referente en la promoción, defensa y garantía de los derechos humanos; privacidad, protección de datos personales, libertad de expresión, acceso a la información, salud, educación y trabajo en el ciberespacio.

Un organismo que en forma centralizada, con personal capacitado y material adecuado, busque estrechar los vínculos con instituciones educativas (nuevo conocimiento), empresas de seguridad informática (intercambio de información en materia de ciberseguridad), especialistas y defensores de derechos humanos (evaluar las prácticas de vigilancia de las comunicaciones para que sean consistentes con los derechos humanos de los usuarios en la red). Un organismo que podría presidir la Secretaria de Gobernación a través de la Subsecretaria de Derechos Humanos que tiene por misión vigilar la legalidad de los actos en que tenga injerencia la Secretaría; impulsar una política de respeto y promoción de los derechos humanos en el ámbito de la Administración Pública Federal, y difundir los ordenamientos jurídicos nacionales, con la finalidad de propiciar el cumplimiento de los preceptos constitucionales.

Lo anterior, permitirá crear una doctrina mexicana en materia de derechos humanos en el ciberespacio, además de impulsar acciones para promover una política pública. Del mismo modo, que la jurisprudencia alemana, ha reconocido que, el derecho a la autodeterminación de la información es inherente al derecho general de la personalidad, a la luz de las nuevas tecnologías, la información y la comunicación.

La segunda propuesta está dirigida hacia la recién conformada Subcomisión de Inteligencia Artificial y *Deep Learning*, un organismo

que colabora en la transformación digital de la política del más alto nivel, al profundizar la innovación, llevar más beneficios a la población con servicios de calidad y avanzar en materia de ciberseguridad, mediante la creación y el mejoramiento de los protocolos de conectividad.

Es a través del Protocolo de Internet Versión 6 (IPV6) que algunas dependencias de la Administración Pública Federal como; las Secretarías de Economía, Salud, Hacienda y Crédito Público, Comunicaciones y Transportes, y Desarrollo Social, colaboran en la simplificación y optimización de los trámites y servicios. Por ejemplo, la digitalización de trámites como: la Clave Única de Registro de Población (CURP), el acta de nacimiento y la cédula profesional, que ya se pueden adquirir a través de internet.

No obstante, los desafíos continuaran como consecuencia de las transformaciones y los retos que se vislumbran para el futuro son fortalecer y mejorar los procedimientos en contrataciones e impedir las conductas fuera de la ley, para así garantizar las buenas prácticas.

Por ello, la República de Estonia, líder en gobernanza digital, sistemas educativos para las TIC y autenticación digital de la identidad. Pionera en el Documento Nacional de Identidad (DNI electrónico), la plataforma X-Road y la firma digital. Referente en la implementación del voto por Internet, ya en 2005, y también del voto por teléfono móvil, en las elecciones de 2008. Creador de la primera embajada digital y promotor del reconocimiento a la libre circulación de datos como la quinta libertad del mercado único de la Unión Europea.

Es la nación referente para proponer el principio a sólo una vez proporcionar información a la Administración Pública, es decir, que ninguna dependencia gubernamental pueda solicitarle a una persona información que haya proporcionado a cualquier otra institución. El propósito es evitar el robo de identidad y el mal uso de los datos personales. Así mismo, se recomienda incluir en el Protocolo de Internet Versión 6 (IPV6), un mecanismo que registre todo acceso a los datos personales y permita que los individuos utilicen el portal de servicios públicos a fin de vigilar y ver qué dependencia consultó sus datos.

Esta práctica favorecería el control individual sobre cómo se utilizan nuestros datos personales, además, podríamos visualizar que servidor público consulta los datos y conocer cuál es propósito. Más aún, en circunstancias extraordinarias iniciar un procedimiento de reclamación de protección de datos, sí algún ciudadano sospecha que se ha violado su derecho a la privacidad. Similar al portal web www.wwsti.ee del que ya se benefician los ciudadanos de Estonia. De ahí, la necesidad de un organismo que vele por los derechos humanos en el ciberespacio, haciendo especial énfasis en la anterior propuesta.

La última propuesta está considerada con la intención de proveer a México de las herramientas necesarias para afrontar las futuras problemáticas en materia de derechos digitales con la mayor asertividad y una adecuada cooperación internacional, puesto que, las soluciones puramente nacionales, serán insuficientes frente a la dimensión internacional que caracteriza a los ciberdelitos.

Es importante recordar que ciberseguridad, no necesariamente, significa la protección de los derechos humanos. Por ello, es necesario encauzar a México en la búsqueda de alianzas estratégicas con naciones afines a sus intereses en el ciberespacio y crear una estrategia internacional para los derechos humanos en el Ciberespacio.

Teniendo en cuenta que, la política aplicada por la República Federativa de Brasil, contribuyó y reformó las instituciones de gobernanza global responsables de la seguridad en las comunicaciones electrónicas, al presentar un proyecto sobre el derecho a la privacidad en la era digital, ante el Consejo de Derechos Humanos de las Naciones Unidas (CDH), en donde, la resolución fue crear la figura del Relator Especial sobre el derecho a la Privacidad. Y, simultáneamente modificó su legislación nacional con el Marco Civil de Internet (Marco Civil da Internet) o Ley de Privacidad en Internet, una legislación que impone límites a los metadatos que pueden ser recolectados de los usuarios de la red en Brasil. Además de exonerar a los proveedores de servicios de Internet de responsabilidad por el contenido publicado por sus usuarios y exigirles cumplir las órdenes judiciales para retirar material ofensivo.

Se ha tomado como referente al país sudamericano para proponer, la posible adhesión de México al Convenio sobre Ciberdelincuencia o Convenio de Budapest, considerado el primer tratado internacional que busca regular los delitos cometidos a través de Internet y otras redes informáticas (entró en vigor el 1 de julio de 2004). El objetivo de este instrumento internacional, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. Entre los estados que son parte se puede mencionar Estados Unidos, Rusia, Francia, Alemania y Estonia.

La escasa respuesta del gobierno mexicano ante las ciberamenazas entre las que destaca el ciberespionaje, porque detrás de él suele haber Estados, expone la falta de desarrollo en las políticas de ciberseguridad mexicanas, si bien existe inversión en dependencias principalmente de seguridad nacional, falta una adecuada investigación en materia de derechos humanos en el ciberespacio.

Al cierre de esta investigación, falta por responder a múltiples preguntas que aún está en el tintero: ¿Cuáles son los requisitos que deben cumplir las empresas prestadoras de servicios de software para ser contratado por la Administración Pública Federal de México? ¿Qué agencia investigó a las empresas Microsoft, Google y Oracle que se han visto involucradas en los programas de espionaje de la NSA? ¿Cuáles son los estándares para auditar las herramientas tecnológicas? ¿Cuál es la regulación para comercializar tecnologías y productos para la vigilancia? ¿Cuáles serían las acciones que México aplicaría ante la eventualidad de que hackeen sus sistemas electorales como ha ocurrido con Rusia y Estados Unidos? ¿Cuáles son los referentes internacionales para considerar que la intervención de comunicaciones proporciona un resultado efectivo y eficiente en materia de seguridad?

Por ello, es importante que los estados, México en particular, considere de conformidad con sus tradiciones jurídicas, su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible al

espionaje electrónico; delimitando las acciones realizadas por medio de las tecnologías de la información y comunicación con respecto a los derechos de los individuos.

CONCLUSIONES

Durante la elaboración de esta investigación, se consultaron las definiciones disponibles del término espionaje electrónico (ciberespionaje), por tanto, se concluye que, las exposiciones del concepto son acotadas, al considerar el estudio del espionaje estatal someramente. Es importante enfatizar que, son los gobiernos de los diferentes países, mediante sus Servicios de Inteligencia o Departamentos de Defensa, quienes violan el derecho a la privacidad en línea de ciudadanos nacionales y extranjeros que no son responsables de ningún hecho ilícito con la finalidad de salvaguardar la seguridad nacional.

Es imperante recordar que, el ciberespionaje es una de las actividades más difíciles de demostrar, puesto que, no se puede determinar si es un Estado el que ataca a otro o si son individuos que realizan actividades antisociales con el propósito de obtener un beneficio. Por ello, es imperante proteger el derecho a la privacidad en línea mediante leyes y políticas más fuertes.

Por otra lado, el resultado del análisis de las políticas públicas en materia de espionaje electrónico (ciberespionaje), empleadas por las seis naciones que han actuado como ejemplo en esta investigación. Se concluye que, la existente regulación internacional del espionaje electrónico bajo el nombre de vigilancia electrónica encierra consecuencias negativas para los individuos porque los gobiernos, especialmente los más poderosos y avanzados tecnológicamente, amparados en la visión tradicional de seguridad nacional, en donde, el Estado sigue siendo el actor principal y el uso de la fuerza el instrumento fundamental, han hecho del ciberespionaje una práctica generalizada.

Es por esto que, las medidas de ciberseguridad deberían contemplar los derechos humanos de cuarta generación, especialmente, el derecho a la privacidad en línea (incluso cuando la seguridad nacional se encuentra en riesgo, la vigilancia electrónica debe ser de uso excepcional y estrictamente delimitado), para el adecuado comportamiento de los Estados en Internet, y la sinergia entre los intereses de seguridad y la privacidad en línea. De ahí que, exista la necesidad

del trabajo conjunto de los Estados para elaborar un marco regulatorio internacional de la vigilancia en el ciberespacio, puesto que la problemática transgrede las fronteras nacionales a medida que la vigilancia electrónica se expande y se vuelve universal. Es decir, se requiere una serie de normas internacionales que permitan a los Estados proteger a sus ciudadanos de las amanezcas internas y externas, y que, al mismo tiempo, respeten y velen por sus derechos.

Las anteriores afirmaciones admiten innumerables cuestionamientos, no obstante, sólo se dará respuesta a la hipótesis formulada al inicio de esta investigación, sí las instituciones garantes de la seguridad nacional en México se han caracterizado por la práctica generalizada para recopilar información (espionaje), consecuencia de su estrecha relación con el sistema político. La actual regulación del delito de espionaje en México, ¿es consecuente con los avances tecnológicos y el impacto que tienen las ciberamenzas, en particular, el ciberespionaje, al modificar el concepto de espacio o ámbito en el que se manifiestan, profundizan y desarrollan los derechos humanos?

En el ámbito nacional mexicano, el artículo 16 constitucional prescribe ciertas protecciones aisladas sobre aspectos relacionados con la privacidad, como lo es, el hecho de que nadie puede ser molestado en su persona, familia, domicilio, papales o posesiones sino en virtud de una orden escrita firmada por una autoridad competente. Por consiguiente, ni la jurisprudencia ni la doctrina mexicanas ha acuñado algún concepto relacionado con este derecho en el sentido expuesto; a lo sumo, sólo ha recogido los avances alcanzados en otras jurisdicciones. Como resultado, en nuestro país no existe ninguna ley específica que regule el ciberespionaje como política pública que involucre a los ciudadanos.

No obstante, en junio de 2009 se incorporó al mismo artículo constitucional, el derecho a la protección de los datos personales y la correlativa facultad que toda persona tiene para acceder, rectificar, cancelar u oponerse a la divulgación de dichos datos. Sí bien este derecho, en sí mismo, no agota el derecho a la privacidad (este incluye a aquel), la incorporación constitucional representa un

avance importante en el orden jurídico mexicano, pues ha sentado las bases para el desarrollo conceptual del derecho a la privacidad.

El 22 de noviembre de 2018, el Senado de la República aprueba la desaparición del CISEN y es sustituido por el Centro Nacional de Inteligencia, el cual tiene funciones del Sistema Nacional de Protección Civil.

El 11 de noviembre de 2018, el coordinador del Grupo Parlamentario del Partido Encuentro Social, Fernando Manzanilla presentó ante el pleno de la Cámara de Diputados una iniciativa de reforma para castigar el espionaje telefónico.

En conclusión, se requiere una adecuada comprensión sobre el impacto de la vigilancia electrónica, en el deterioro del derecho a la privacidad en línea y otros derechos humanos.

Hoy en día cualquier persona que tenga un dispositivo conectado a internet —también un vehículo, cualquier dispositivo doméstico o incluso una casa inteligente—, alguien, o varios a la vez, puede estar recopilando todo tipo de información, tanto sobre quién lo usa como para qué —lo que permite conocer costumbres, aficiones y vicios—, y sin tener la certeza de cuándo, hasta qué extremo y con qué consecuencias podrá ser empleada esa información en nuestro perjuicio. Además, la mayoría de nosotros difundimos en las redes sociales lo que pensamos, soñamos, aborrecemos, etc. Sin la necesidad de que quien recopila la información (personas, grupos, empresas, Estados) recurran al ciberespionaje.

Por lo cual, la privacidad desaparece cuando nos conectamos a Internet o hacemos una llamada telefónica, y las leyes nacionales de privacidad, así como las normas internacionales, no logran seguir el ritmo de los cambios tecnológicos.

La aprensión que sienten los gobiernos hacia las nuevas tecnologías y concretamente internet, por amplificar las amenazas a las que se enfrentan. Los ha llevado a intensificar las medidas de ciberseguridad; emitiendo decretos o proponiendo leyes para obligar a las empresas de tecnología a entregar los datos de sus usuarios y decodificar las comunicaciones, los cortafuegos nacionales, el

bloqueo generalizado de medios sociales e incluso el cierre total de Internet, son tácticas empleadas por gobiernos represivos para controlar la actividad en línea. Medidas contradictorias y que son en detrimento del derecho a la privacidad en línea. Medidas judiciales conminatorias (las personas que publican contenidos controvertidos en Internet, regularmente no tienen los recursos necesarios para oponerse a ordenes estatales) que pretenden eliminar las expresiones artísticas, heterodoxia, crítica y debate.

Existe una divergencia generalizada entre lo que dicen los estados (manifiestan en foros internacionales, su compromiso de observar los derechos humanos en línea) y lo que hacen efectivamente (adoptar leyes que cercenan tales derechos, indicando que lo hacen por la seguridad de sus ciudadanos). Un escenario que expone la necesidad observar la forma, en que los gobiernos protegen los derechos en la era digital (internet no debería ser utilizado como excusa, para indicar que los derechos humanos son menos importantes o queden sujetos a estándares completamente diferentes a los existen fuera del mismo).

Por tanto, cuando los Estados introducen restricciones a los derechos humanos se debe demostrar su necesidad (debe demostrar que existe una conexión directa e indirecta, entre el derecho objeto de restricción y la amenaza) y adoptar únicamente las medidas que resulten proporcionales a la consecución de los legítimos objetivos (seguridad nacional, el orden público o los derechos de terceros) para lograr una protección constante y eficaz de los derechos.

Por ejemplo, la justificación más habitual para emplear la vigilancia electrónica y legitimar cualquier restricción es la seguridad nacional (aspiración que debería entenderse como el interés público, más que el interés de un determinado gobierno o élite). Así que, la vigilancia electrónica indiscriminada es una medida difícil de justificar como necesaria, porque la limitación de un derecho, debe ser por el medio menos restrictivo y es complicado imaginar que invadir regularmente la privacidad de todas las personas y monitorear las comunicaciones de todos pueda ser proporcional a una amenaza concreta, incluso cuando la amenaza representa un movimiento terrorista.

Sabemos que los derechos humanos son respetados cuando existe transparencia en la legislación y en las prácticas del estado, supervisión independiente de las facultades ejecutivas y posibilidades de apelación y resarcimiento. De modo que, cada país debe asegurar que las personas puedan utilizar estas tecnologías, sin temor a intromisiones invasivas y desproporcionadas en su vida privada asegurando la transparencia, la rendición de cuentas y la democracia en el mundo.

FUENTES CONSULTADAS

BIBLIOGRAFÍA

Acuña H., Carlos (2013). *¿Cuánto importan las instituciones?: Gobierno, Estado y Actores en la política argentina*, Buenos Aires, Edit. Siglo XXI, 398pp.

Aguayo Quezada, Sergio y Bailey, John (1997), (coord.). *Las seguridades de México y Estados Unidos en un momento de transición*, México, Edit. Siglo XXI, 346pp.

Aguayo Quezada, Sergio y Bailey, Bruce M. (1990), (comp.). *En busca de la Seguridad Perdida, Aproximaciones a la Seguridad Nacional Mexicana*, México, Edit. Siglo XXI, 412pp.

Angulo, Jacovo (2014). *Seguridad Nacional y Derechos Humanos en México (1917- 2008)*, México, Edit. INACIPE, 365pp.

Arreola García, Adolfo (2015). *Ciberespionaje: la puerta al mundo virtual de los Estados e individuos*, México, Edit. Siglo XXI, 250pp.

Bobbio, Norberto, Matteucci, Nicola y Pasquino, Gianfranco (1991). *Diccionario de Política*, México, Edit. Siglo XXI, 872pp.

Buendía, Manuel (1996). *La CIA en México*, México, Edit. Rayuela, 271pp.

Del Castillo, Arturo (1996). *El nuevo institucionalismo en el análisis organizacional: conceptos y enunciados explicativos*, México, Edit. Centro de Investigación y Docencia Económicas (CIDE), 34pp.

González García, Juan (2009). *Teoría del desarrollo económico neoinstitucional una alternativa a la pobreza en el siglo XXI*, México, Edit. Porrúa, 154pp.

Hinley, F.H. (1972). *"El concepto de soberanía"*, Barcelona, Edit. Nueva Colección Labor, 146pp.

Jiménez, René y Silva Forné, Carlos (2016). *Los mexicanos vistos por sí mismos. Los grandes temas nacionales. Percepción del desempeño de las instituciones de seguridad y justicia*, México, Edit. UNAM, 186pp.

Piñeyro, José Luis (2006). *Seguridad Nacional en México: ¿realidad o proyecto?*, Barcelona-México, Edit. Pomares, 205pp.

Tapia Valdés, Jorge A. (1980). *El terrorismo de Estado. La Doctrina de la Seguridad Nacional en el cono sur*, México, Edit. Nueva Imagen, 283pp.

Romero, Jorge Javier (2010). *Para entender: Las Instituciones Políticas*, México, Edit. Nostra Ediciones, 77pp.

Segura Serrano, Antonio, Gordo García, Fernando (2013). *Ciberseguridad global oportunidades y compromisos en el uso del ciberespacio*, España, Edit. Universidad de Granada, 243pp.

Tocora, Fernando (1995). *Política Criminal en América Latina Seguridad Nacional y Narcotráfico*, México, Edit. Orlando Cárdenas, 226pp.

PÁGINAS ELECTRÓNICAS

Abad Liñán José Manuel. *Anonymus anuncia su mayor ataque informático contra el Estado Islámico.* En http://tecnologia.elpais.com/tecnologia/2015/11/16/actualidad/1447689267_713343.html (consultada el 02 de mayo de 2017).

Abellaán Lucía y Pérez Claudi. *Atentado en Bruselas: al menos 30 muertos en el aeropuerto y el metro.* En https://elpais.com/internacional/2016/03/22/actualidad/1458631407_286826.html (consultada el 23 de marzo de 2018).

Acta final de la Segunda Conferencia Internacional de la Paz. En https://archivos.juridicas.unam.mx/www/bjv/libros/3/1158/6.pdf (consultada el 02 de agosto de 2018).

Afghan War Diary. En https://wikileaks.org/afg/ (consultada el 16 de abril de 2017).

Ahmed Azam. *Investigadores del GIEI dicen que fueron espiados para entorpecer la investigación del caso Ayotzinapa.* En

https://www.nytimes.com/es/2017/07/10/pegasus-giei-espionaje-ayotzinapa/ (consultada el 25 de octubre de 2017).

Alcántara, Liliana. *Posibilidad de ejecución en Tlatlaya: ONU.* En http://archivo.eluniversal.com.mx/primera-plana/2014/impreso/posibilidad-de-ejecucion-en-tlatlaya-onu-47032.html (consultada el 18 de octubre de 2017).

Alessi, Gil. *La justicia de Brasil bloquea una vez más WhatsApp.* En https://elpais.com/tecnologia/2016/05/02/actualidad/1462203263_150504.html (consultada el 01 de agosto de 2017).

Álvarez, Caro María. *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital.* En https://books.google.com.mx/books?id=kRSyCQAAQBAJ&pg=PA96&lpg=PA96&dq=alemania+derecho+a+la+privacidad&source=bl&ots=l9SXIdCtgN&sig=SIyEiZ9WQwqhrj1UJZSAB9uZDtg&hl=es&sa=X&ved=0ahUKEwjgrYrEysbVAhWK7iYKHWp4Aj0Q6AEIXTAJ#v=onepage&q&f=false (consultada el 14 de agosto de 2017).

Álvarez, Eduardo. *Francia ordena a Microsoft que deje de espiar en Windows 10.* En http://computerhoy.com/noticias/software/francia-ordena-microsoft-que-deje-espiar-windows-10-48456 (consultada el 30 de julio de 2017).

Angwin, Julia *et al*. *AT&T Helped U.S. Spy on Internet on a Vast Scale.* En https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html (consultada el 03 de agosto de 2017).

ANSSI. En https://translate.google.com.mx/translate?hl=es-419&sl=en&u=https://www.ssi.gouv.fr/en/&prev=search (consultada el 30 de abril de 2017).

Aprueba Senado Ley General del Sistema Nacional Anticorrupción. En http://comunicacion.senado.gob.mx/index.php/informacion/boletines/29206-aprueba-senado-ley-general-del-sistema-nacional-anticorrupcion.html (consultada el 19 de octubre de 2017).

Archivos de la Stasi: el rompecabezas más grande del mundo. En http://www.bbc.com/mundo/noticias/2012/09/120916_cultura_documentos_archivos_stasi_bd (consultada el 09 de agosto de 2017).

Article 9. En https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006419288 (consultada el 26 de julio de 2017).

Artículo 16 Constitucional. En http://207.249.17.176/Transparencia/XIV%20Transp%20y%20Acceso%20Inform%20Marco%20normativo/Articulo%2016%20Constitucional.pdf (consultada el 27 de junio de 2017).

Atentados en Paris causan 150 muertos. En http://www.jornada.unam.mx/2015/11/14/politica/002n1pol (consultada el 01 de mayo de 2017).

Autodeterminación Informativa. En http://www.informatica-juridica.com/trabajos/autodeterminacion-informativa/ (consultada el 15 de agosto de 2017).

Barragán, Sebastián. *Licitaciones a modo benefician a empresarios cercanos a Peña Nieto.* En http://aristeguinoticias.com/0905/mexico/licitaciones-a-modo-benefician-a-empresarios-cercanos-a-pena-nieto/ (consultada el 24 de octubre de 2017).

Beauregard, Luis Pablo. *EL Gobierno mexicano declaró secretos los contratos sobre el software del espionaje a periodistas.* En https://elpais.com/internacional/2017/06/20/mexico/1497984473_017962.html (consultada el 25 de octubre de 2017).

Becerril, Andrés. *El de Buendía, el primer crimen de narcopolítica.* En http://www.excelsior.com.mx/nacional/2014/05/30/962316 (consultada el 29 de octubre de 2017).

Berdah, Arthur. *Loi renseignement: les écolos décrochent leur télephone pour rallier les députés.* En http://www.lefigaro.fr/politique/le-scan/2015/05/04/25001-20150504ARTFIG00184-loi-renseignement-les-ecolos-decrochent-leur-telephone-pour-rallier-les-deputes.php (consultada el 01 de agosto de 2018).

Bortnik, Sebastián. *Troyanos y gusanos: el reinado del malware Análisis de las 100 amenazas más detectadas por ESET en Latinoamérica*. En http://www.welivesecurity.com/wp-content/uploads/2014/01/troyanos-y-gusanos-el-reinado-del-malware.pdf (consultada 22 de abril de 2016).

Brasil aumenta su presupuesto militar para garantizar la seguridad en los Juegos. En https://www.infodefensa.com/latam/2016/07/20/noticia-diferentes-agencias-seguridad-brasilenas-defenderan-juegos.html (consultada el 21 de marzo de 2018).

Brasil, eventos de 2016. En https://www.hrw.org/es/world-report/2017/country-chapters/298774 (consultada el 02 de agosto de 2017).

Brito, Diana. *Polícia do Rio prende 19 manifestantes na véspera da final da Copa.* En http://www1.folha.uol.com.br/poder/2014/07/1485042-policia-civil-prende-19-suspeitos-de-vandalismo-no-rio.shtml (consultada el 21 de marzo de 2018).

Bundesdatenschutzgesetz (BDSG). En http://www.wipo.int/wipolex/es/text.jsp?file_id=328201 (consultada el 14 de agosto de 2017).

Capítulo II: El Estado y su origen. En http://catarina.udlap.mx/u_dl_a/tales/documentos/ledf/priego_s_g/capitulo2.pdf (consultada el 20 de mayo de 2017).

Carta de los Derechos Fundamentales de la Unión Europea. En http://www.europarl.europa.eu/charter/pdf/text_es.pdf (consultada el 14 de agosto de 2017).

Case of Roman Zakharov vs Russia (Application no. 47143/06). En http://www.statewatch.org/news/2015/dec/echr-russian-secret-surveillance-judgment.pdf (consultada el 12 de julio de 2017).

Charlie Hebdo attack: Three days of terror. En http://www.bbc.com/news/world-europe-30708237 (consultada el 30 de abril de 2017).

Chelsea Manning, libre. En http://www.jornada.unam.mx/2017/05/18/opinion/002a1edi (consultada el 28 de junio de 2017).

Chilling Effects: NSA Surveillance Drive U.S. Writers to Self-Censor. En https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (consultada el 13 de marzo de 2018).

Constitución de la Federación Rusa. En https://archivos.juridicas.unam.mx/www/bjv/libros/1/186/4.pdf (consultada el 10 de marzo de 2018).

Constitución Política de los Estados Unidos Mexicanos. En http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf (consultada el 16 de noviembre de 2017).

Contreras Vega, Gerardo, Ochoa Rivera, Carlos A. y Solís Muñiz, Adolfo de Jesús. *Introducción a la seguridad en Internet y aplicaciones***.** En http://www.capacinet.gob.mx/Cursos/Tecnologia%20amiga/desarrolladordesoftware/Seguridad_Internet_SE.pdf (consultada el 22 de abril de 2016).

Convención Americana sobre Derechos Humanos. En http://www.acnur.org/fileadmin/scripts/doc.php?file=fileadmin/Documentos/BDL/2001/0001 (consultada el 17 de abril de 2017).

Convención de Viena sobre Relaciones Diplomáticas. En http://www.cndh.org.mx/DocTR/2016/JUR/A70/01/JUR-20170331-II14.pdf (consultada el 27 de septiembre de 2017).

Convenio Europeo de Derechos Humanos. En http://www.echr.coe.int/Documents/Convention_SPA.pdf (consultada el 14 de agosto de 2017).

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. En http://www.echr.coe.int/Documents/Convention_SPA.pdf (consultada el 17 de abril de 2017).

Coyne, Christopher J. *Review of Glennon.* En http://www.ccoyne.com/Review_of_Glennon.pdf (consultada el 30 de julio de 2018).

Cumbre del consumidor G20. En https://translate.google.com.mx/translate?hl=es-419&sl=en&u=http://unctad.org/en/pages/MeetingDetails.aspx%3Fmeetingid%3D1355&prev=search (consultada el 23 de marzo de 2018).

Curzio, Leonardo. *Estado, soberanía y seguridad nacional*. En http://www.cisan.unam.mx/pdf/lc02_03.pdf (consultada el 17 de mayo de 2107).

Declaración Universal de Derechos Humanos. En http://www.acnur.org/t3/fileadmin/scripts/doc.php?file=t3/fileadmin/Documentos/BDL/2001/0013 (consultada el 16 de abril de 2017).

Décret n°2007-1527 du 24 octobre 2007 relatif au droit de réponse applicable aux services de communication au public en ligne et pris pour l'application du IV de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. En https://www.legifrance.gouv.fr/affichTexte.do;?cidTexte=JORFTEXT000000428279 (consultada el 30 de julio de 2017).

Decreto por el que se aprueba la Convención Interamericana sobre Personalidad y Capacidad de Personas Jurídicas en el Derecho Internacional Privado. En http://www.dof.gob.mx/nota_detalle.php?codigo=4638093&fecha=06/02/1987 (consultada el 27 de septiembre de 2017).

Decreto promulgatorio del Acuerdo entre los Estados Unidos Mexicanos y la República de Guatemala sobre cooperación para combatir el narcotráfico y la farmacodependencia. En http://dof.gob.mx/nota_detalle.php?codigo=4653865&fecha=04/03/1992&print=true (consultada el 27 de septiembre de 2017).

Decreto promulgatorio del Tratado de Cooperación Mutua entre el Gobierno de los Estados Unidos Mexicanos y el Gobierno de la República de Guatemala para el Intercambio de Información respecto de Operaciones Financieras. En http://www.dof.gob.mx/nota_detalle.php?codigo=698258&fecha=05/03/2003 (consultada el 27 de septiembre de 2017).

De la Corte Ibáñez Luis y Blanco Navarro. *Seguridad nacional, amenazas y respuestas.* En https://books.google.com.mx/books?id=qkBsBQAAQBAJ&pg=PT139&lpg=PT139&dq=ciberdefensa+francia&source=bl&ots=1TYC6noWXr&sig=sVLx0saW6CQoBSD

6H_t2dgPndCg&hl=es-419&sa=X&ved=0ahUKEwiEmfj-sM3TAhWQ14MKHZKUD7k4ChDoAQhLMAc#v=onepage&q=ciberdefensa%20francia&f=false (consultada el 30 de abril de 2017).

Devinat, Mathieu y Guilhermont, Édith. *La reception des théories juridiques francaises en droit civil québécois.* En https://www.usherbrooke.ca/droit/fileadmin/sites/droit/documents/RDUS/volume_42/42-3-Devinat-Guilhermont.pdf (consultada el 27 de julio de 2017).

Digitaalallkirja seadus. En https://www.riigiteataja.ee/akt/694375 (consultada el 20 de agosto de 2017).

Doncel, Luis. *Un hombre mata a 12 personas con un camión en Berlín y reaviva el miedo al terrorismo en Europa.* En https://elpais.com/internacional/2016/12/19/actualidad/1482176155_449814.html (consultada el 23 de marzo de 2018).

Duarte, Javier. En http://aristeguinoticias.com/tag/javier-duarte/ (consultada el 19 de octubre de 2017).

Editorial: Cuando los gobiernos no se resisten a abusar de los programas espía. En https://www.nytimes.com/es/2017/07/11/editorial-programas-espia-mexico-pegasus-gobiernoespia/ (consultada el 30 de octubre de 2017).

El derecho a la privacidad en la era digital. En https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/11/PDF/G1707311.pdf?OpenElement (consultada el 06 de agosto de 2017).

Electronic Communications Privacy Act of 1986 (ECPA). En https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (consultada el 05 de julio de 2017).

El espionaje no es un asunto menor: Carlos Loret de Mola (Video). En http://aristeguinoticias.com/1906/mexico/el-espionaje-no-es-un-asunto-menor-carlos-loret-de-mola-video/ (consultada el 19 de octubre de 2017).

El ministerio de Economía francés, víctima de un gran ataque informático. En http://www.elmundo.es/elmundo/2011/03/07/internacional/1299480465.html (consultada el 01 de mayo de 2017).

Elola, Joseba. *Un hombre en el centro del huracán.* En http://elpais.com/diario/2010/12/26/domingo/1293339155_850215.html (consultada el 16 de abril de 2017).

Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed. En https://www.riigiteataja.ee/akt/120032013007 (consultada el 20 de agosto de 2017).

Esparza, Pablo. *¿Qué es el Estado de emergencia y por qué Francia lo mantiene 12 meses después de los ataques de París?* En http://www.bbc.com/mundo/noticias-internacional-37966286 (consultada el 01 de mayo de 2017).

Europa reconoce el derecho al olvido en Internet. En http://www.lanacion.com.ar/1690239-europa-reconoce-el-derecho-al-olvido-en-internet (consultada el 30 de julio de 2017).

Executive Order 12333. En https://www.cia.gov/about-cia/eo12333.html (consultada el 05 de julio de 2017).

Experto de la ONU pide a EE UU que mejore la protección de la información privada. En http://www.un.org/spanish/News/story.asp?NewsID=37603#.WVxL4RU1-1s (consultada el 04 de julio de 2017).

Expertos de la ONU consideran arbitraria la detención de Julian Assange. En http://www.un.org/spanish/News/story.asp?NewsID=34385#.WVMNEpI1-1s (consultada el 27 de junio de 2017).

Fazio, Carlos. *Tanhuato: la barbarie y la impunidad.* En http://www.jornada.unam.mx/2016/08/29/opinion/018a1pol (consultada el 19 de octubre de 2017).

Fernández, Rodrigo. *Estonia, primera víctima de los 'hackers'.* En https://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html (consultada el 20 de agosto de 2017).

Fierro, Juan Omar. *Pegasus tuvo al menos seis responsables en PGR, entre 2014 y 2016.* En http://aristeguinoticias.com/0307/mexico/pegasus-tuvo-seis-responsables-en-pgr-entre-octubre-de-2014-y-2016/ (consultada el 09 de octubre de 2017).

Foreingn Intellingencce Surveillance Court. En http://www.fisc.uscourts.gov/ (consultada el 17 de marzo de 2018).

Fox – Brewster Thomas. *NSO Group: Los espías israelíes que hackean iPhones con un solo SMS.* En https://www.forbes.com.mx/nso-group-los-espias-israelies-que-hackean-iphones-con-un-solo-sms/ (consultada el 08 de octubre de 2017).

Francia: Gobierno vigilará llamadas y datos de internet con nueva ley, denuncia AI. En http://aristeguinoticias.com/2407/mundo/francia-gobierno-vigilara-llamadas-y-datos-de-internet-con-nueva-ley-denuncia-ai/ (consultada el 03 mayo de 2017).

Frente Mexiquense acusa a PGJEM: tortura, fabrica delitos y carpetas de investigación. En http://www.proceso.com.mx/439688/frente-mexiquense-acusa-a-pgjem-tortura-fabricar-delitos-carpetas-investigacionn (consultada el 24 de octubre de 2017).

García González, Aristeo. *La protección de datos personales: Derecho Fundamental del siglo XXI. Un estudio comparado*. En http://www.ejournal.unam.mx/bmd/bolmex120/BMD000012003.pdfv (consultada el 16 de mayo de 2017).

García, Paula G. *Francia da tres meses a Facebook para cumplir con la Ley de Protección de Datos.* En http://www.expansion.com/empresas/tecnologia/2016/02/09/56b9d3c422601d637e8b4649.html (consultada el 30 de julio de 2017).

Garrido, Antonio y Parra, Francisco. *Nuevo Institucionalismo y Políticas Públicas*. En http://www.aecpa.es/uploads/files/congresos/congreso_09/grupos-trabajo/area06/GT01/08.pdf (consultada el 20 de mayo de 2016).

Glennon, Michael J. *National Security and Double Government.* En http://harvardnsj.org/wp-content/uploads/2014/01/Glennon-Final.pdf (consultada el 04 de julio de 2017).

Global Network Initiative; protecting and advancing freedom of expression and privacy in information and communications technologies. En https://www.globalnetworkinitiative.org/international/Espanol.php (consultada el 29 de junio de 2017).

Gobierno espía, vigilancia sistemática a periodistas y defensores de derechos humanos en México. En https://articulo19.org/wp-content/uploads/2017/06/Reporte-Gobierno-Espi%CC%81a-Final.pdf (consultada el 09 de octubre de 2017).

Greenwald, Glenn. *The NSA´s mas and indiscriminate spying on Brazilians.* En https://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying (consultada el 02 de agosto de 2017).

Greenwald, Glenn, Kaz Roberto y Casado José. *EUA espionaram milhões de e-mails e ligações de brasileiros.* En https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934 (consultada el 02 de agosto de 2017).

Guerrero, Claudia. *Entran ciudadanos a debatir Ley 3de3.* En http://www.reforma.com/aplicacioneslibre/articulo/default.aspx?id=812139&md5=5da1733bc52731710eec3e373d947d99&ta=0dfdbac11765226904c16cb9ad1b2efe&lcmd5=ac9e7b9ce8e96066b5ed38c876dc33e4 (consultada el 23 de octubre de 2017).

Guerrero Peralta, Oscar Julián. *La expectativa razonable de intimidad y el derecho fundamental a la intimidad en el proceso penal*. En http://revistas.uexternado.edu.co/index.php/derpen/article/viewFile/2961/2605 (consultada el 15 de mayo de 2017).

Hädaolukorra seadus. En https://www.riigiteataja.ee/akt/13201475 (consultada el 20 de agosto de 2017).

Hackean tienda de PlayStation de Sony en internet. En http://www.bbc.com/mundo/ultimas_noticias/2014/12/141208_ultnot_tecnologia_sony_ataque_cibernetico_lv (consultada el 08 de mayo de 2017).

H.R.2048-USA Freedom Act of 2015. En https://www.congress.gov/bill/114th-congress/house-bill/2048/text (consultada el 07 de marzo de 2018).

Hugo, Grocio. En https://archivos.juridicas.unam.mx/www/bjv/libros/6/2698/11.pdf (consultada el 03 de septiembre de 2017).

Informe de seguimiento del Relator Especial sobre la tortura y otros tratos o penas crueles, inhumanos o degradantes – México. En http://www.hchr.org.mx/images/doc_pub/InformeSeguimientoRelatorONUTortura2017.pdf (consultada el 18 de octubre de 2017).

Informe de Transparencia. En https://transparencyreport.google.com/government-removals/by-country/RU (consultada el 10 de marzo de 2018).

Informe Mundial 2017: Estados Unidos. En https://www.hrw.org/es/world-report/country-chapters/298275 (consultada el 16 de abril de 2017).

Inquiétude des Organisations des Droits de L´homme face á un Projet de Loi Visant á donner aux Agences de Renseignement de nouveaux pouvoirs qui ne sont pas sans danger. En https://www.ldh-france.org/inquietude-organisations-droits-lhomme-face-projet-loi-visant-donner-aux-agences-renseignement-nouveaux-pouvoirs-pas-danger/ (consultada el 15 de marzo de 2018).

Iraq War Logs. En https://wikileaks.org/irq/ (consultada el 17 de abril de 2017).

Isikuandmete kaitse seadus. En https://www.riigiteataja.ee/akt/106012016010 (consultada el 20 de agosto de 2017).

Jauvert, Vincent. *Comment la France écoute (aussi) le monde.* En https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html (consultada el 15 de marzo de 2018).

Jiménez González, Claudia G. *Las teorías de la cooperación internacional dentro de las relaciones internacionales*. En http://www.juridicas.unam.mx/publica/librev/rev/polis/cont/20032/art/art5.pdf (consultada el 29 de marzo de 2016).

Kasperskylab. *Grupo Equation: El creador principal del ciberespionaje*. En https://latam.kaspersky.com/about/press-releases/2015_grupo-equation-el-creador-principal-del-ciberespionaje (consultada el 22 de abril de 2016).

Katz vs. United States, 389 U.S. 347 (1967). En https://supreme.justia.com/cases/federal/us/389/347/case.html (consultada el 07 de marzo de 2018).

La casa blanca de Enrique Peña Nieto (investigación especial). En http://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/ (consultada el 23 de octubre de 2017).

La Constitución de los Estados Unidos de América 1787. En https://www.archives.gov/espanol/constitucion.html (consultada el 03 de julio de 2017).

La Presidencia del Consejo de la UE. En http://www.consilium.europa.eu/es/council-eu/presidency-council-eu/ (consultada el 17 de agosto de 2017).

La responsabilidad de las empresas de respetar los derechos humanos. En http://www.ohchr.org/Documents/Publications/HR.PUB.12.2_sp.pdf (consultada el 29 de junio de 2017).

La Rue Frank,Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. En http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (consultada el 07 de mayo de 2017).

Legisladores renuevan programa para espiar a extranjeros fuera de EU. En https://aristeguinoticias.com/1101/mundo/legisladores-renuevan-programa-para-espiar-a-extranjeros-fuera-de-estados-unidos/ (consultada el [en 27 de marzo de 2018).

Lei Nº 12.965, de 23 de abril de 2014. En http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (consultada el 31 de julio de 2017).

Lemos, Ronaldo. *Artigo: Internet brasileira precisa de marco regulatório civil.* En https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm (consultada el 06 de agosto de 2017).

Ley de Seguridad Nacional. En http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf (consultada el 22 de abril de 2016).

Ley Federal de Transparencia y Acceso a la Información Pública. En http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf (consultada el 27 de octubre de 2017).

Ley Federal N° 149-FZ, de 27 de julio de 2006, sobre Información, Tecnologías de la Información y Protección de la Información (en su versión modificada por la Ley Federal N° 222-FZ de 21 de julio de 2014. En http://www.wipo.int/wipolex/es/details.jsp?id=15688 (consultada el 10 de marzo de 2018).

Ley Fundamental de la República Federal de Alemania. En https://www.btg-bestellservice.de/pdf/80206000.pdf (consultada el 15 de agosto de 2017).

Libran cargos por traición periodistas del blog Netzpolitik en Alemania (Video). En http://aristeguinoticias.com/1108/mundo/liberan-cargos-por-traicion-periodistas-de-blog-netzpolitik-en-alemania-video/ (consultada el 12 de agosto de 2017).

Litovkin, Nikolai. *Las cibertropas rusas, entre las mejores del mundo.* En https://es.rbth.com/tecnologias/defensa/2017/01/11/las-cibertropas-rusas-entre-las-mejores-del-mundo_678818 (consultada el 17 de julio de 2017).

Loi du 24 juillet 2015 relative au renseignement. En http://www.vie-publique.fr/actualite/panorama/texte-discussion/projet-loi-relatif-au-renseignement.html (consultada el 30 de julio de 2017).

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1). En https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676 (consultada el 30 de julio de 2017).

Loi n° 2008-3 du 3 janvier 2008 pour le développement de la concurrence au service des consommateurs (1). En https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000017785995 (consultada el 30 de julio de 2017).

Loi n° 2008-696 du 15 juillet 2008 relative aux archives. En https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019198529 (consultada el 30 de julio de 2017).

Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (1). En https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte (consultada el 15 de marzo de 2018).

Luhn, Alec. *El Gran Hermano ruso: el país aprueba una ley que reduce las libertades y la privacidad.* En https://www.eldiario.es/theguardian/Gran-Hermano-aprueba-libertades-privacidad_0_531247722.html (consultada el 10 de marzo de 2018).

Madden, Mary. *Public Perceptions of provacy and Seciritu in the Post-SnowdeN Era.* En http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (consultada el 07 de marzo de 2018).

Manual General de Organización de la Secretaría de Marina. En https://www.gob.mx/cms/uploads/attachment/file/200287/MANUAL_GENERAL_DE_ORGANIZACION_DE_LA_SEMAR.pdf (consultada el 11 de octubre de 2017.

Manual de Organización General de la Secretaría de Gobernación. En http://www.diputados.gob.mx/LeyesBiblio/regla/n205.pdf (consultada el 17 de septiembre de 2017).

Manual de Organización General de la Secretaría de la Defensa Nacional. En https://www.gob.mx/cms/uploads/attachment/file/48566/M.O.F._Secretar_a_de_la_Defensa_Nacional.pdf (consultada el 10 de octubre de 2017).

Marcial Pérez, David. *Una filtración revela el uso de hackers por el Gobierno mexicano.* En https://elpais.com/internacional/2015/07/07/actualidad/1436220111_034556.html (consultada el 25 de octubre de 2017).

Markoff, John. *Georgia sufre guerra cibernética.* En https://elpais.com/diario/2008/08/14/internacional/1218664803_850215.html (consultada el 19 de julio de 2017).

Márquez, William. *Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU.* En http://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm (consultada el 26 de marzo de 2017).

Martínez Jiménez, Clara. *El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia.* En https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/1222/TFG000913.pdf?sequence=1 (consulta el 11 de julio de 2017).

McGuinness, Damien. *El caso de libertad de expresión que causa conmoción en Alemania.* En http://www.bbc.com/mundo/noticias/2015/08/150806_libertad_de_expresion_alemania_lb (consultada el 10 de agosto de 2017).

Méndez, Ernesto. *Renuncia David Korenfels como director de Conagua.* En http://www.excelsior.com.mx/nacional/2015/04/10/1017862 (consultada el 24 de octubre de 2017).

Meraz, Andrea. *Urge INAI a gobierno crear política de ciberseguridad.* En https://www.excelsior.com.mx/nacional/2017/05/18/1164313 (consultada el 20 de agosto de 2018).

Moraes, Camila. *Un juez ordena bloquear WhatsApp en todo el territorio brasileño.* En https://elpais.com/internacional/2016/07/19/actualidad/1468941131_714293.html (consultada el 01 de agosto de 2017).

Moran Espinosa, Alejandra, Servín Caamaño, Abraham Alejandro y Alquicira Gálvez, Óscar. *TIC (Internet) y Ciberterrorismo – III*. En https://revista.seguridad.unam.mx/node/2223 (consultada el 23 de marzo de 2017).

Nájar, Alberto. *Kiki Camarena, el caso que México no puede olvidar.* En http://www.bbc.com/mundo/noticias/2013/08/130821_enrique_kiki_camarena_salazar_caso_dea_narcotrafico_mexico_caro_quintero_an (consultada el 29 de octubre de 2017).

National Cyber Investigative Joint Task Force. En https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force (consultada el 05 de julio de 2017).

National Security Act of 1947. En https://history.state.gov/milestones/1945-1952/national-security-act (consultada el 05 de julio de 2017).

National Security Agency. En https://www.nsa.gov/ (consultada el 05 de julio de 2017).

Observaciones generales aprobadas por el Comité de Derechos Humanos. En https://conf-dts1.unog.ch/1%20SPA/Tradutek/Derechos_hum_Base/CCPR/00_2_obs_grales_Cte%20DerHum%20%5BCCPR%5D.html (consultada el 03 de julio de 2017).

Olmstead vs. United States, 277 U.S. 438 (1928). En https://supreme.justia.com/cases/federal/us/277/438/case.html (consultada el 07 de marzo de 2018).

ONU: Internet es un derecho humano. En http://archivo.eluniversal.com.mx/articulos/64522.html (consultada el 07 de mayo de 2017).

Ordaz, David. *Pagó gobierno de México 15 millones de dólares a firma de ciberespionaje: NYT.* En http://aristeguinoticias.com/0309/mexico/pago-gobierno-de-mexico-15-millones-de-dolares-a-firma-de-ciberespionaje-nyt/ (consultada el 25 de octubre de 2017).

Pacto Internacional de Derechos Civiles y Políticos. En http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx (consultada el 17 de abril de 2017).

Paga Sedena 5 mmdp por equipo para espiar. En http://archivo.eluniversal.com.mx/notas/859221.html (consultada el 25 de octubre de 2017).

Page, David. *¿Por qué Estonia quiere ser líder mundial en ciberdefensa?* En http://www.expansion.com/2014/09/09/empresas/tecnologia/1410254908.html (consultada el 20 de agosto de 2017).

Panama papers: Criminales, políticos y los negocios turbios que esconden sus fortunas. En http://aristeguinoticias.com/tag/panama-papers/ (consultada el 24 de octubre de 2017).

Pastor Acosta, Óscar, Pérez Rodríguez José Antonio, Arnáiz de la Torre Daniel y Taboso Ballesteros Pedro. *Seguridad Nacional y Ciberdefensa.* En http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf (consultada el 13 de julio de 2017).

Patrón Sánchez, Mario. *La crisis de derechos humanos que nos alcanzó.* En http://www.proceso.com.mx/466497/la-crisis-derechos-humanos-nos-alcanzo (consultada el 19 de octubre de 2017).

Pegasus: el software espía definitivo para iOS y Android. En http://www.eluniversal.com.mx/articulo/techbit/2017/04/20/pegasus-el-software-espia-definitivo-para-ios-y-android (consultada el 08 de octubre de 2017).

Peirano, Marta. *Esta muñeca ha sido prohibida en Alemania por espiar a los niños.* En http://www.eldiario.es/cultura/privacidad/muneca-prohibida-Alemania-espiar-ninos_0_615938787.html (consultada el 09 de agosto de 2017).

Pereda, Cristina F. *Estados Unidos "decepcionado" por el dictamen contra el envió de datos.* En https://elpais.com/internacional/2015/10/06/actualidad/1444154032_422524.html (consultada el 30 de julio de 2017).

PLUSD The Public Library of US Diplomacy. En https://wikileaks.org/plusd/ (consultada el 17de abril de 2017).

Purdy, Matthew. *The making of a suspect: the case of Wen Ho Lee.* En https://www.nytimes.com/2001/02/04/us/the-making-of-a-suspect-the-case-of-wen-ho-lee.html (consultada el 30 de julio de 2018).

Programa para la Seguridad Nacional 2014 - 2018. En http://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014 (consultada el 09 de octubre de 2017).

Prohíben la venta de una muñeca espía en Alemania. En http://www.milenio.com/internacional/muena_espia-mi_amiga_cayla-alemania-

prohiben_venta-espiar_ninos_0_904709828.html (consultada el 09 de agosto de 2017).

Promueve INAI Derecho a la Privacidad de las personas. En http://www.lja.mx/2017/01/promueve-inai-derecho-a-privacidad-las-personas/ (consultada el 20 de agosto de 2018).

Propósitos y Principio de las Naciones Unidas. En http://www.un.org/es/sc/repertoire/principles.shtml (consultada el 28 de agosto de 2017).

Qué es lo que Estados Unidos espía a sus aliados. En http://www.bbc.com/mundo/noticias/2015/06/150624_wikileaks_eeuu_internacional_espionaje_por_que_aliados_se_espian_ig (consultada el 02 de mayo de 2017).

¿Qué es una APT? En https://blog.kaspersky.es/que-es-una-apt/966/ (consultada el 07 de mayo de 2017).

¿Qué es y qué no un hacker? En http://www.egov.ufsc.br/portal/sites/default/files/cdn_hacking_v2.pdf (consultada el 23 de abril de 2017).

Quem defende seus datos? En http://quemdefendeseusdados.org.br/pt/ (consultada el 20 de marzo de 2018).

¿Qué son los derechos humanos? En http://www.ohchr.org/SP/Issues/Pages/WhatareHumanRights.aspx (consultada el 07 de mayo de 2017).

Ramírez Millán, Jesús. *Teoría del Estado*. En https://archivos.juridicas.unam.mx/www/bjv/libros/3/1461/5.pdf (consultada el 17 de mayo de 2017).

Rebollo Delgado, Lucrecio. *Vida privada y protección de datos: un acercamiento a la regulación internacional europea y española*. En https://archivos.juridicas.unam.mx/www/bjv/libros/6/2758/10.pdf (consultada el 03 de septiembre de 2017).

Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional. En http://www.diputados.gob.mx/LeyesBiblio/regla/n18.pdf (consultada el 09 de octubre de 2017).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). En

https://www.boe.es/doue/2016/119/L00001-00088.pdf (consultada el 23 de marzo de 2018).

Reston, James. *La seguridad absoluta para una nación es la inseguridad para todas las demás.* En https://elpais.com/diario/1977/01/21/internacional/222649219_850215.html (consultada el 04 de marzo de 2018).

Reséndiz, Francisco. *No hay pruebas de espionaje por parte del gobierno: Presidencia.* En http://www.eluniversal.com.mx/articulo/nacion/politica/2017/06/19/no-hay-pruebas-de-espionaje-por-parte-del-gobierno-presidencia (consultada el 25 de octubre de 2017).

Resoluciones aprobadas sobre la base de los informes de la sexta comisión. En http://www.un.org/es/comun/docs/?symbol=A/RES/2625(XXV)&Lang=S&Area=RESOLUTION (consultada el 28 de agosto de 2017).

Riigisaladuse ja salastatud välisteabe seadus. En https://www.riigiteataja.ee/akt/RSVS (consultada el 20 de agosto de 2017).

Rivas Leone, José Antonio. *El neoinstitucionalismo y la revalorización de las instituciones.* En http://www.redalyc.org/articulo.oa?id=11000903 (consultada el 22de marzo de 2017).

Robinson, Andy. *Amigos y enemigos de la Gestapo.* En http://www.lavanguardia.com/cultura/20160823/404136394894/frank-mcdonough-gestapo-colaboracion-multinacionales-regimen-nazi.html (consultada el 10 de agosto de 2017).

Ros, Elianne. *¿Cómo gestionar el derecho a la muerte digital?* En http://www.lavanguardia.com/vida/20160229/4085405270/francia-regula-tratamiento-post-mortem-datos-internet.html (consultada el 30 de julio de 2017).

Rothtock, Kevin. *En Rusia, empresas de internet llevan a juicio al Kremlin por vigilancia en línea.* En http://www.elespectador.com/tecnologia/rusia-empresas-de-internet-llevan-juicio-al-kremlin-vig-articulo-620054 (consultada el 11 de julio de 2017).

Rusia / Georgia: *Todas las partes del conflicto de Osetia del Sur en agosto violaron las leyes de la guerra.* En https://www.hrw.org/es/news/2009/01/23/rusia/georgia-todas-las-partes-del-conflicto-de-osetia-del-sur-en-agosto-violaron (consultada el 18 de julio de 2017).

Russian military admits significant cyberwar effort. En http://www.bbc.com/news/world-europe-39062663 (consultada el 17 de julio de 2017).

Saiz, Eva. *El soldado Manning, condenado a 35 años por las filtraciones a Wikileaks.* En http://internacional.elpais.com/internacional/2013/08/21/actualidad/1377090640_718161.html (consultada el 16 de marzo de 2017).

Sánchez Pérez, Gabriel y Rojas González, Isai. *Leyes De Protección de Datos Personales en el Mundo y la Protección de Datos Biometricos - Parte I.* En https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93 (consultada el 09 de agosto de 2017).

Sandoval Castellanos, Edgar Jair. *Ingeniería Social: corrompiendo la mente humana.* En https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana (consultada el 02 de agosto de 2018).

Sanger David, E. *Obama order sped up wave of ciberattacks against Iran.* En https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?hp (consultada el 26 de julio de 2018).

Seguridad Nacional. En https://www.hrw.org/es/united-states/seguridad-nacional (consultada el 27 de marzo de 2018).

Shame on France: French Constitutional Council Widely Approves Surveillance Law. En https://www.laquadrature.net/en/shame-on-france-french-constitutional-council-widely-approves-surveillance-law (consultada el 15 de marzo de 2018).

Shaw, Jonathan. *The Wachers: Assaults on privacy in America.* En https://harvardmagazine.com/2017/01/the-watchers (consultada el 29 de marzo de 2018).

Shedler, Andreas. *Neoinstitucionalismo*. En https://books.google.com.mx/books?id=QK79r_mPPG8C&pg=PA472&lpg=PA472&dq=Las+instituciones+sociales+son+creaciones+sociales;+no+son+ni+hechos+naturales+ni+productos+divinos:+el+origen+social+de+las+instituciones.&source=bl&ots=Ll7wrhOC7N&sig=btX5FIUfdHX3wMRkx1TQSiPoyWM&hl=es-419&sa=X&ved=0ahUKEwiBp66kLMAhUh2oMKHeK1AUQQ6AEIGjAA#v=onepage&q=Las%20instituciones%20sociales%20son%20creaciones%20sociales%3B%20no%20son%20ni%20hechos%20naturales%20ni%20productos%20divinos%3A%20el%20origen%20social%20de%20las%20instituciones.&f=false (consultada el 22 de mayo de 2016).

Son necesarios límites para proteger la privacidad en el ciberespacio. En http://www.un.org/spanish/News/story.asp?newsID=30954#.WRETsUU1-1s (consultada el 08 de mayo de 2017).

Sparrow, Thomas. *El efecto inesperado del discurso de Obama sobre el espionaje.* En

http://www.bbc.com/mundo/noticias/2014/01/140116_eeuu_obama_anuncio_nsa_analisis_tsb (consultada el 27 de marzo de 2018).

Strategy for Informatión Society Development until 2030 approved. En http://en.kremlin.ru/acts/news/54477 (consultada el 09 de marzo de 2018).

Supervisor europeo de protección de datos. En https://edps.europa.eu/sites/edp/files/publication/17-05-23_opinion_etias_ex_summ_es.pdf (consultada el 24 de marzo de 2018).

Telemediengesetz. En https://www.lmk-online.de/fileadmin/user_upload/Bilder/01_Die_LMK/06_Rechtsgrundlagen/Telemediengesetz_2016.pdf (consultada el 15 de agosto de 2017).

Teruel, Ana. *Francia reconoce el derecho a desconectar del trabajo.* En https://elpais.com/tecnologia/2017/01/03/actualidad/1483440318_216051.html (consultada el 30 de julio de 2017).

The Cyber Intelligence Sharing and Protection Act, H.R. 624. En https://democrats-intelligence.house.gov/sites/democrats.intelligence.house.gov/files/documents/cispaonepager.pdf (consultada el 06 de julio de 2017).

The hunt for the dawn of APTSs: a 20 year-old atttack that remains relevant. En https://www.kaspersky.com/about/press-releases/2017_the-hunt-for-the-dawn-of-apts-a-20-year-old-attack-that-remains-relevant (consultada el 13 de julio de 2017).

Thielman, Sam y Ackerman, Spencer. *Cozy Bear and Fancy Bear: did Russians hack Democratic party and if so why?* En https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc (consultada el 13 de Julio de 2017).

Thomas, Lupita. *Hechos en Nochixtlan dejan 6 muertos y 21 detenidos.* En http://www.eluniversal.com.mx/articulo/estados/2016/06/19/hechos-en-nochixtlan-dejan-6-muertos-y-21-detenidos (consultada el 24 de octubre de 2017).

Toledo, María José. *Putin aprueba una nueva doctrina para la seguridad de información rusa.* En http://rtw24.com/putin-aprueba-una-nueva-doctrina-para-la-seguridad-de-informacion-rusa/ (consultada el 11 de julio de 2017).

Tratado Americano de Soluciones Pacíficas. En http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-42_soluciones_pacificas_pacto_bogota.asp (consultada el 27 de septiembre de 2017).

UKUSA Agreement Release 1940-1956. En https://www.nsa.gov/news-features/declassified-documents/ukusa/ (consultada el 05 de julio de 2017).

United States vs. Jeffrey Sterling. En https://law.justia.com/cases/federal/appellate-courts/ca4/11-5028/11-5028-2013-10-16.html (consultado el 13 de marzo de 2018).

United States vs. John Kiriakou. En https://www.justice.gov/archive/opa/documents/kiriakou-complaint.pdf (consultada el 13 de marzo de 2018).

United States vs. Jones, 565 U.S. 400 (2012). En https://supreme.justia.com/cases/federal/us/565/400/ (consultada el 07 de marzo de 2018).

United States vs. Leibowitz. En https://www.courtlistener.com/docket/4285776/united-states-v-leibowitz/ (consultada el 13 de marzo de 2018).

United States vs. Thomas Andrews Drake. En https://fas.org/sgp/jud/drake/plea.pdf (consultada el 13 de marzo de 2018).

Un niño de cinco años logra hackear una cuenta de Xbox. En http://www.excelsior.com.mx/hacker/2014/04/04/952325 (consultada el 08 de mayo de 2017).

U.S. Cyber Command (USCYBERCOM). En http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (consultada el 05 de julio de 2017).

U.S. STRATEGIC COMMAND. En http://www.stratcom.mil/ (consultada el 05 de julio de 2017).

Vela, Luis. *El Derecho Natural en Giorgio del Vecchio*. En https://books.google.com.mx/books?id=ebyyd7UUGewC&pg=PA68&lpg=PA68&dq=giorgio+del+vecchio+la+soberania&source=bl&ots=6m0U29ru-d&sig=MoKeWS18csH6qrT4hn5dBubC7YY&hl=es&sa=X&ved=0ahUKEwiosemSoYrWAhXC4yYKHT9eAFUQ6AEIXDAO#v=onepage&q&f=false (consultada el 03 de septiembre de 2017).

Vigilancia y democracia: historias en 10 países. En https://www.cels.org.ar/web/wp-content/uploads/2017/06/Vigilancia-y-democracia_INCLO.pdf (consultada el 19 de marzo de 2018).

Villegas, Paulina. *Me quitaron la mitad de mi vida: el dolor de las mujeres de Atenco, diez años después.* En https://www.nytimes.com/es/2016/09/22/me-quitaron-la-mitad-de-mi-vida-el-dolor-de-las-mujeres-de-atenco-diez-anos-despues/ (consultada el 18 de octubre de 2017).

Visita al Brasil del Ministro de Asuntos Exteriores de Noruega, Borge Brende - Río de Janeiro y Brasilia, 19 y 20 de febrero de 2014. En http://www.itamaraty.gov.br/es/notas-a-la-prensa/3580-visita-al-brasil-del-ministro-de-asuntos-exteriores-de-noruega-borge-brende-rio-de-janeiro-y-brasilia-19-y-20-de-febrero-de-2014 (consultada el 06 de agosto de 2017).

Visita del Ministro de Relaciones Exteriores a Alemania – Berlín, 21 de marzo de 2014. En http://www.itamaraty.gov.br/es/notas-a-la-prensa/3556-visita-del-ministro-de-relaciones-exteriores-a-alemania-berlin-21-de-marzo-de-2014 (consultada el 06 de agosto de 2017).

Vita, Leticia. *Soberanía y derecho internacional en el pensamiento jurídico de Weimar*. En http://www.derecho.uba.ar/investigacion/investigadores/publicaciones/vita-soberania-y-derecho-internacional-en-el-pensamiento-juridico-de-weimar.pdf (consultada el 03 de septiembre de 2017).

Warren, Samuel D. y Brandeis, Louis D. *The Right to Privacy*. En http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (consultada el 03 de julio de 2017).

Yárnoz, Carlos. *El espía más indiscreto de Francia.* En https://elpais.com/internacional/2016/09/03/actualidad/1472893224_106150.html (consultada el 15 de marzo de 2018).