UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE DERECHO

EL ESTABLECIMIENTO DE LÍMITES A LA CONSERVACIÓN DE DATOS PERSONALES POR PARTE DE LOS CONCESIONARIOS DE TELECOMUNICACIONES

TESIS

Que para obtener el título de

ESPECIALIDAD EN DERECHO DE LA INFORMACIÓN

P R E S E N T A

AGUSTIN GRANADOS TZINTZUN

DIRECTORA DE TESIS

DRA. EUGENIA PAOLA CARMONA DÍAZ DE LEÓN

Ciudad Universitaria, Cd. Mx., 2018

EL ESTABLECIMIENTO DE LÍMITES A LA CONSERVACIÓN DE DATOS PERSONALES POR PARTE DE LOS CONCESIONARIOS DE TELECOMUNICACIONES

INTRODUCCIÓN 4

CAPITULO PRIMERO: MARCO TEORICO-CONCEPTUAL 9

1. Conceptos 11

a) Vigilancia Estatal: 11

b) Intervención de las comunicaciones: 12

c) Metadatos 12

d) Derecho a la Intimidad 13

e) Seguridad Nacional 14

I. Ley de Seguridad Nacional 16

II. Ley General del Sistema de Seguridad Pública 17

III. Diferencias Seguridad Nacional y Seguridad Pública: 18

a) Autodeterminación informativa 19

b) Vigilancia y Datos Personales 20

2. Libertad de expresión 21

3. Libertad de Expresión en Internet: principios orientadores 22

4. Limitaciones a la libertad de expresión 24

5. Derecho a la Privacidad 29

6. Privacidad de las Comunicaciones 33

CAPÍTULO SEGUNDO. DISPOSICIONES LEGALES EN MATERIA DE CONSERVACIÓN Y PROTECCIÓN DE DATOS PERSONALES. 35

1. Ley Federal de Telecomunicaciones y Radiodifusión 35

2. Posicionamiento sobre la inconstitucionalidad del artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión..... 36

a) Comisionada Areli Cano Guadiana 38

b) Oscar Mauricio Guerra Ford..... 40

3. Lineamientos de Colaboración en Materia de Seguridad y Justicia 42

4. Ley Federal de Protección de Datos Personales en Posesión de los Particulares..... 47

Principios de la LFPDPPP..... 48

- Principio de licitud 48
- Principio de consentimiento 49
- Principio de información..... 52
- Principio de calidad 54
- Principio de finalidad 55
- Principio de lealtad..... 55
- Principio de proporcionalidad..... 56
- Principio de responsabilidad 57
- Deber de confidencialidad y seguridad 58
- Derechos ARCO 59

5. Convención Interamericana de Derechos Humanos..... 61

6. Directiva 2006/24/CE Del Parlamento Europeo 65

7. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo..... 67

8. Sentencia del Tribunal de Justicia Europeo 69

CAPÍTULO TERCERO. LA CONSERVACIÓN DE DATOS PERSONALES EN MÉXICO 74

1. Conservación de los Datos Personales de acuerdo a la Ley Federal de Telecomunicaciones y Radiodifusión..... 74

2. Excepciones a la privacidad 77
3. Jurisprudencia SCJN 80
4. Conflictos de interés 84
5. Estadísticas 90
a) Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2016 91
b) Estadísticas Red en Defensa de los Derechos Digitales 93
CAPÍTULO CUARTO. LÍMITES A LA CONSERVACIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS CONCESIONARIOS DE TELECOMUNICACIONES 95
1. Limitaciones a la vigilancia 95
a) Ley Previa 97
b) Proporcionalidad y necesidad 97
2. Órgano revisor a las solicitudes de vigilancia 100
3. Seguridad de los Datos Personales 104
a) La Directiva 2002/58/CE del Parlamento Europeo 105
4. Eliminación de los datos personales conservados 107
5. Garantías a la Libertad de Expresión por parte del Estado 107
CONCLUSIONES 109
BIBLIOGRAFIA Y CIBERGRAFÍA 112
Libros 112
Revistas 115
Cibergrafía 116
Jurisprudencia 118

INTRODUCCIÓN

Considero que el uso de programas o sistemas de vigilancia en las comunicaciones privadas debe ser utilizado en forma excepcional, y como parte de ello en cuestiones de seguridad pública con la finalidad de preservar el orden y la paz pública. Esta ha sido la nueva tendencia en donde la seguridad pública y seguridad nacional, es la justificación constante de los gobiernos.

Es por ello que cuando hablamos de la actual evolución y desarrollo de las tecnologías de la información, nos encontramos ante la gran capacidad de almacenamiento de una infinidad de datos personales sobre una misma persona, en donde se pueden obtener catálogos de datos, ya sea que se encuentren en bases de datos diferentes, en lugares distintos, toda la información sobre las personas se puede acumular sin limitaciones y obtenerse en cuestión de segundos sin importar la localización física.

Respecto al área de telecomunicaciones, existe la implementación de programas y prácticas de seguridad, como el almacenamiento obligatorio de los datos personales de los usuarios por parte de los concesionarios de servicios de telecomunicaciones a partir de la entrada en vigor de la Ley Federal de Telecomunicaciones y Radiodifusión el 14 de agosto de 2014.

Esto puede afectar la libertad de expresión, cualquier persona al saber que su comportamiento o cualquier forma de expresión es observada se ve intimidado y por lo tanto es razonable sentir la perdida de la privacidad[1].

[1] *Cfr.* Relator Especial de la Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Libertad de Expresión y Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*, disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2 consultado el 17 de noviembre de 2017

En consecuencia, se modifica lo que se piensa o dice, porque creemos que estamos haciendo algo malo o porque no se desea llamar la atención de instituciones del gobierno o evitar que malas interpretaciones de lo que decimos e incluso en donde nos localizamos o hasta con quienes nos comunicamos, es evidente que la vigilancia a los medios de comunicación es un acto que tiene un efecto inhibidor que afecta el derecho a la privacidad y la libertad de expresión.[2]

Es importante señalar que todas estas innovaciones de las tecnologías de la información, en el área de las telecomunicaciones y contenidos digitales tienen una influencia no solo en lo tecnológico, también influyen en el cambio social y en las formas de convivencia.

En este sentido, actualmente se establece la obligación a los concesionarios de telecomunicaciones al tratamiento y conservación de datos personales de acuerdo al artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión (en lo sucesivo LFTR)[3].

---

[2] *Cfr.* Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Libertad de Expresión e Internet*. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf consultado el 17 de noviembre de 2017, p. 73

[3] **Artículo 190.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

[…]

II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

a) Nombre, denominación o razón social y domicilio del suscriptor;

b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

En efecto, se dispone la obligación de los concesionarios de telecomunicaciones de conservar información personal de todos los usuarios, de cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad. Así como la conservación por 12 meses que permitan su consulta y entrega en tiempo real y conservarla por 12 meses más en dispositivos que permitan su consulta, sin señalar excepciones o sin justificar un tiempo extremadamente excesivo de 24 meses.

---

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

Para tales efectos, el concesionario deberá **conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes**, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos **por doce meses adicionales en sistemas de almacenamiento electrónico**, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

[…]

(***Énfasis añadido)***

Es por ello que en el presente trabajo tratamos de exponer ¿Por qué es violatorio de derechos humanos? ¿Por qué se deben implementar medidas para que el uso no sea generalizado?, así como proponer mecanismos para la evitar la vulneración a la privacidad y la protección de datos personales por parte de las autoridades y los concesionarios de telecomunicaciones.

También, mencionaremos la forma en que se viola los principios a la protección de datos personales, y con ello se pretende realizar un análisis sobre las posibles propuestas que limiten el uso excesivo de las autoridades en la conservación de datos.

Nuestra hipótesis no consiste restringir el acceso a los datos conservados por los concesionarios de telecomunicaciones, sino en establecer mecanismos previos para evitar las autoridades sin indicios, pruebas o motivos que acrediten fehacientemente la comisión de un delito practiquen en forma indiscriminada solicitudes de acceso a datos conservados y que terminan en abusos de autoridad que violan los derechos humanos de los ciudadanos.

Se utilizó el derecho comparado en gran medida porque en los tratados internacionales de los que México es parte ha aceptado la jurisdicción dela Corte Interamericana de Derechos Humanos en lo sucesivo la CIDH. Asimismo, la protección de datos personales tiene su origen y evolución en Europa, nuestro país no solo retoma los principios de datos sino la autodeterminación como un derecho de decidir sobre y tratamiento de nuestros personales. Sin olvidar la serie de obligaciones de los responsables en el uso, almacenamiento, divulgación etc., de los datos personales.

El derecho a la protección de datos en Europa se ha manifestado en contra de la conservación de datos personales y ha declarado que es violatorio de derechos humanos el tratamiento de datos en forma general y además que no se garantiza la

correcta actuación de las autoridades sin la existencia de una instancia revisora, así como tampoco se garantiza la destrucción de la información.

En nuestro primer capítulo, hacemos una referencia a los conceptos relativos y específicos a la materia de protección de datos y derechos fundamentales que son utilizados durante todo el trabajo.

En el segundo capítulo señalamos las disposiciones vigentes en materia de conservación de datos y la protección de datos personales, así como el derecho comparado con la legislación europea.

El tercer capítulo señalamos a la conservación de datos en forma específica en la LFTR, con el posicionamiento sobre el tema por parte de la Suprema Corte de Justicia de la Nación (en lo sucesivo la SCJN); por otra parte, señalamos los resultados y estadísticas sobre la protección de datos personales y la eficacia de las solicitudes de conservación de datos de las autoridades.

Por último, el cuarto capítulo comprende las limitaciones que consideramos deben ser utilizadas frente a las autoridades previo a las solicitudes, y evitar la conservación de datos por un periodo excesivo a los concesionarios de telecomunicaciones y que afecta en forma general a todos los usuarios de telecomunicaciones.

CAPITULO PRIMERO: MARCO TEORICO-CONCEPTUAL

La información representa un mecanismo para el desarrollo de las naciones tanto el aspecto social como económico, algunos consideran que conforme a la globalización es importante tener el dominio de la información para la conformación de los poderes[4].

Aun se realizan cambios de manera constante en el uso de la tecnología, lo cual modifica nuestra forma de relacionarnos o nuestra forma de vida, esto no solo es utilizado por las personas, también los gobiernos, empresas. Se habla cada día más del uso del computó en la nube, también encontramos al *big data* que contiene enormes cantidades de información o la nueva tendencia de los llamados datos abiertos que son datos de carácter público en posesión del gobierno, lo cuales deben estar accesibles en línea con la finalidad de que puedan ser reutilizados y redistribuidos por cualquier interesado.

Por otra parte, incluso el buen uso o el aspecto positivo en el manejo de las Tecnologías de la Información y Comunicación en lo sucesivo (TIC), tiene riesgos para las personas, por ello la existencia del espionaje comercial o con cualquier fin, también existen los ataques informáticos, el robo de identidad, los contenidos ilícitos como pedofilia, abuso sexual, por señalar algunos casos[5].

Las personas somos titulares del derecho a la protección de datos, las normativas actuales protegen a todas las personas frente al tratamiento ya sea de sector privado o del sector público. Las personas tienen un derecho subjetivo y en ese

[4] Navarro Isla, Jorge (Coord), *Tecnologías de la Información y de las Comunicaciones: Aspectos Legales,* México, Porrúa, 2005, p. 14

[5] Ornelas Nuñez, Lina Gabriela y Alcalde Urbina, Samantha, *La protección de datos personales de menores en la era digital,* México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2014, p. 10.

sentido no se trata de proteger los datos sino de la protección de la persona y la información que él lo identifica[6].

De acuerdo a la Constitución Política de los Estados Unidos Mexicanos en lo sucesivo la CPEUM, la protección de datos personales es un derecho fundamental, que involucra a todas las personas y por el cual tenemos como titulares el derecho a que sea respetado por los responsables en el tratamiento sea el sector privado o el sector público[7].

El derecho a la autodeterminación no es ilimitada como sucede con otros derechos, se puede describir a la autodeterminación informativa como la capacidad que tenemos para decidir sobre quién y cuáles son los datos que autorizamos sean utilizados, así como, las finalidades en donde señalamos de forma específica para que objetivo entregamos nuestros datos personales[8].

Se hace referencia a la protección de datos porque como lo señalamos en capítulos posteriores, no encontramos ante un caso de excepción en donde por mandato de ley, los concesionarios de telecomunicaciones se encuentran obligados al almacenamiento de la información, sin embargo, no se han cumplido las formalidades que la misma ley establece y que claramente violan los principios de protección de datos.

Para del desarrollo del presente trabajo es necesario describir algunos conceptos a lo que haremos referencia además de contextualizarlos a nuestra materia.

---

[6] Comisión para el Acceso a la Información Pública y Protección de Datos et. al, *Transparentemente: Protección de Datos Personales*, Retos a la Protección de Datos en un mundo globalizado, Isabel Davara Fernández de Marcos, México, Comisión para el Acceso a la Información Pública y Protección de Datos (Puebla), 2012, p. 30

[7] Ibidem, p. 31

[8] Remolina Angarita, Nelson, *Tratamiento de datos personales: Aproximación Internacional y comentarios a la Ley 1581 de 2012,* Colombia, 2013, p. 29

1. Conceptos

En términos generales cuando hablamos de conservación de datos personales, nos encontramos ante una parte de parte de la vigilancia estatal, la cual puede en algunos casos ser justificada en cuestiones de seguridad y que solo debería ser realizada mediante autorización judicial. De hecho, la conservación de datos personales ha sido nombrada como parte de la colaboración con las autoridades judiciales.

Dentro de los conceptos necesarios para el desarrollo del tema tenemos los siguientes:

a) Vigilancia Estatal:

Podemos señalar que nosotros escogimos una definición de la Asociación Red en Defensa de los Derechos Digitales, la consideramos acorde a nuestro tema, por ello el concepto de vigilancia estatal se refiere a la recolección, *almacenamiento*, monitoreo y análisis de información personal llevada a cabo por parte de autoridades públicas o por requerimiento de ellas[9].

De acuerdo a esta pequeña definición en términos generales es cualquier uso sobre la información personal que es *recabada por las autoridades*, en el caso que nos ocupa no la realiza directamente el Estado, sino a través de los concesionarios de telecomunicaciones, los obliga a la guarda de información para su disponibilidad como son; el nombre del suscriptor, el tipo de comunicación, datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía, así como datos para determinar la fecha, hora y duración de la llamada entre otras.

[9] Red en Defensa de los Derechos Digitales, *El Estado de la vigilancia fuera de control*, disponible en: *https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf*, p. 6

De acuerdo a lo anterior toda esa información que se crea cuando usamos bienes, productos o servicios son conocidos como “metadatos” o datos de “tráfico de comunicaciones”.

b) Intervención de las comunicaciones:

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, limita la posibilidad de llevar a cabo la intervención de comunicaciones privadas. Esta posibilidad se contempla, a su vez, en diversas leyes federales.

De acuerdo con el artículo 291 segundo párrafo del Código Nacional de Procedimientos Penales define la intervención de comunicaciones privadas como:

> “La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.”

De acuerdo al artículo 190 de la LFTR, es obligación de los concesionarios de telecomunicaciones colaborar con las instancias de seguridad, procuración y administración de justicia, por lo que la solicitud de intervención solo será procedente mediante mandamiento escrito y fundado por la autoridad competente, de esta forma la intervención de comunicaciones privadas abarca una serie de datos que hagan posible la identificación.

c) Metadatos

Los metadatos son los datos que se generan sobre la comunicación de una persona, los cuales en su conjunto consideramos que son datos personales porque pueden hacer identificable a una persona. Si bien es cierto que determinar la fecha, hora y

duración de una comunicación no es representa un dato personal, si se relaciona con el nombre y domicilio del suscriptor, la ubicación geográfica, el tipo de comunicación (trasmisión de voz, buzón vocal, conferencia, datos), es evidente que se puede identificar a las persona y para efectos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en lo sucesivo la LFPDPPP) así como la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados es un dato personal cualquier información concerniente a una persona física identificada o identificable.

Como ejemplo de los metadatos son: los números telefónicos de origen y destino de una comunicación; la hora, fecha y duración de la misma, la ubicación digital del posicionamiento geográfico de las líneas telefónicas. (art.190 de la LFTyR)

Los metadatos en su conjunto no solo pueden identificar a las personas, sus gustos, sus actividades, sus desplazamientos, así como saber con quienes se relaciona, todo ello puede proporcionar más información personal que el simple contenido de las comunicaciones[10].

d) Derecho a la Intimidad

En términos sencillos, lo íntimo representa los actos que se dejan fuera del conocimiento de otros, aquello que solo se manifiesta a unos cuantos.

La vida **íntima** y privada se ha generado en la misma medida que el poder político ha limitado su obsesión por el control, por ello la libertad frente al poder público, aparece como un conjunto de poderes y facultades para garantizar la exclusión del Estado en el ámbito de las personas.

[10] Gómez-Robledo Verduzco, Alonso y Ornelas Núñez, Lina, *Protección de datos personales en México: el caso del Poder Ejecutivo, México*, Instituto de Investigaciones Jurídicas UNAM, 2006, pp. 13-14.

La concepción del derecho a la **intimidad** se encuentra relacionado con la capacidad de estar solo, la opción de no ser molestado, como una obligación de no hacer[11].

De acuerdo a nuestro tema, la LFTR lo que hace es restringir y tratar de justificar la intervención, la información sobre lo que decidimos hacer en nuestro domicilio, la forma de organizar nuestra vida familiar es asunto privado, y con estas excepciones (geolocalización y conservación de datos) que realiza la autoridad nos encontramos ante una suspensión y una interferencia pública, por lo que como todos los derechos no son absolutos.

La intimidad es un derecho que depende en cierta forma o se determina por cada persona, es por ello que cada quien define que es intimo para él mismo. Se ha considerado que el objeto del *derecho a la protección de datos personales* es mucho más amplio, el derecho a la intimidad sólo comprende dentro de su ámbito los datos de la vida íntima, y el objeto a la protección de datos no solo protege los datos íntimos, sino cualquier dato personal, sea sensible o no, privado o público[12].

e) Seguridad Nacional

Es un término que se asocia a un valor absoluto que el Estado otorgaba para garantizar el orden vigente, con el cual vulneraba los derechos humanos de los ciudadanos[13].

La seguridad nacional ha evolucionado en su concepción y ahora se adapta a un panorama internacional y a las características de un sistema político, es de reconocerse que en México se cambió la normativa y se institucionalizo la

[11] Garriga Domínguez, Ana, *Tratamiento de datos personales y derechos fundamentales*, Madrid España, Dykinson, 2009, p. 20
[12] Comisión para el Acceso a la Información Pública y Protección de Datos, op. Cit., p. 32
[13] Escuela de Inteligencia y Seguridad Nacional (ESISEN), *Inteligencia y Seguridad Nacional*, México, ESISEN, 2009, p. 21

inteligencia y seguridad nacional. Actualmente es una obligación compartida en los poderes y los conceptos se definen en la Ley de Seguridad Nacional, de fecha 19 de diciembre de 2005[14].

De acuerdo con la Constitución Política de los Estados Unidos Mexicanos, no existe una definición particular de la seguridad nacional, sin embargo, es una facultad exclusiva del Congreso de la Unión, tal y como lo señala el artículo 73 fracción XXIX-M, que a la letra dispone lo siguiente:

> […]
> XXIX-M. Para expedir leyes en materia de seguridad nacional, estableciendo los requisitos y límites a las investigaciones correspondientes.
> […]

De acuerdo con la Ley de Seguridad Nacional, no hay concepto claro sino una serie de acciones tendientes a la mantener la integridad, estabilidad y permanencia del país. En lo conducente el artículo 3 señala lo siguiente:

> […]
> Artículo 3.- 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 conlleven a:
> I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país;
> II. La preservación de la soberanía e independencia nacionales y la defensa del territorio;
> III. El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;
> IV. 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;

[14] Ibidem, p. 23

V. La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional, y
VI. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes.
[…]

En todas las ocasiones debería implementarse la obligación en caso de las intercepciones de llamadas o comunicaciones privadas pasen por la autorización de un juez, lo cual ya se encuentra establecido en la ley, respetando los principios de legalidad constitucional.

Por su parte el autor Ernesto Villanueva, considera que históricamente México, tiene un presidencialismo puro en la regulación de la seguridad, el Poder Ejecutivo tiene una primera responsabilidad sobre los servicios de inteligencia para proteger la seguridad nacional, por esto surge la interrogante de ¿cómo asegurar que realmente se cumpla la función de Estado y no una defensa de intereses ajenos?[15]

La seguridad nacional debe referirse a acciones inmediatas reactivas, tácticas y operativas sobre la aplicación de políticas con la finalidad de erradicar un problema, por otra parte, la seguridad nacional se debe limitar estrictamente al objeto de la seguridad y no respecto a los individuos[16].

I. Ley de Seguridad Nacional

Como lo señalamos en La Ley de Seguridad Nacional la define como las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado mexicano como son las siguientes:

[15] Villanueva, Ernesto, *Seguridad nacional, información y poder legislativo,* disponible en https://archivos.juridicas. unam.mx/www/bjv/libros/5/2404/15.pdf, P. 196
[16] Navarro Sánchez, Urenda Queletzú, *Seguridad Nacional: Reformas y Perspectivas*, México, Dirección Generak de Estudios Legislativos, Instituto Belisario Domínguez Senado de la República, 2011, p. 17

- Proteger al país frente a riesgos y amenazas.
- Preservar la soberanía, independencia, territorio y la unidad de la federación.
- Mantener el orden constitucional y fortalecer las instituciones democráticas de gobierno.
- Defender al país frente a otros Estados o sujetos de derecho internacional.
- Preservar el régimen democrático fundado en el desarrollo social, económico y político[17].

De acuerdo a la definición anterior, consideramos que la seguridad nacional, no es una razón para conservar los datos de los concesionarios de telecomunicaciones en forma generalizada, creemos que la conservación de los datos solo debe realizarse sobre quienes exista un temor fundado que representan una amenaza a la seguridad nacional.

En el tema de seguridad nacional debe impedir el uso excesivo de la fuerza, y siempre evitar facultades discrecionales, es decir evitar malos manejos en los procedimientos, con el objetivo real de preservar la seguridad nacional.

II. Ley General del Sistema de Seguridad Pública

La seguridad pública es una función del Estado con la finalidad de salvaguardar la integridad de las personas, conservar el orden y la paz públicos, ello comprende la prevención de los delitos, sanciones administrativas y la readaptación social del sentenciado.

Como se ha señalado el Estado tiene la obligación de desarrollar las políticas para la prevención del delito y por otra parte incentivar una sociedad con valores cívicos y culturales, asimismo los programas son las acciones que pretende realizar el Estado.

[17] Artículo 3 de la Ley de Seguridad Nacional, *http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf*

A diferencia de la seguridad nacional, esta tiene la particularidad de ser necesaria la existencia de una amenaza y que el riesgo sea de tal magnitud que pueda desestabilizar las instituciones, y la seguridad pública se refiere a un peligro concreto que es la delincuencia común[18].

III. Diferencias Seguridad Nacional y Seguridad Pública:

Son conceptos que se relacionan de uno se puede considerar que es consecuencia del otro, la Seguridad Pública es una función que corresponde a los tres niveles de gobierno y tiene como actividades la prevención, investigación y persecución de delitos, así como las sanciones de infracciones administrativas.

Por otra parte, la Seguridad Pública puede convertirse en asunto de Seguridad Nacional en el grado en que el problema criminal represente un riesgo para la integridad, estabilidad y permanencia del Estado, para el orden constitucional, las instituciones democráticas y el desarrollo social, económico y político, en el grado en que constituyan un obstáculo para que las autoridades actúen contra la delincuencia organizada.

De acuerdo a la información del CISEN, la diferencia entre Seguridad Nacional y Seguridad Pública son las siguientes:

Tema	Seguridad Nacional	Seguridad Pública
Objetivos	Tiene como propósito mantener la integridad, estabilidad y permanencia del Estado Mexicano.	Salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos.
Instrumentos	Son la operación de tareas de inteligencia y contrainteligencia para proponer medidas de prevención, disuasión, contención o neutralización de riesgos o amenazas.	Son la prevención, persecución, sanción de las infracciones, así como la reinserción social de las y los delincuentes e infractoras o infractores.

[18] Navarro Sánchez, Urenda Queletzú, op. cit., p. 21

Autoridades responsables	Es materia federal. El Gobierno de la República establece mecanismos de cooperación con las autoridades estatales y municipales.	Es una materia concurrente en la que los tres niveles de gobierno comparten la responsabilidad de la misma en los ámbitos de su competencia.[19]

En el cuadro se hace referencia a la distinción entre los objetivos, los instrumentos y las autoridades que se consideran responsables.

a) Autodeterminación informativa

El tema de la protección de datos personales es considerado un derecho humano en nuestra legislación, y como parte fundamental encontramos a la autodeterminación informativa que es el derecho que tiene cada persona a decidir qué información dar, a cambiar, modificar o suprimir los datos personales que le atañen de cualquier base de datos[20]. Esta protección es extensible a cualquier dato no solo a los datos sensibles, aunque los datos en un inicio no parecieran adecuados o insignificantes, pero que en su conjunto pueden ser usados para finalidades distintas.

Este concepto surge con el Tribunal Constitucional Alemán en 1983, como el derecho esencial en el uso de la información de las personas. Se refiere a la facultad de las personas a decidir cuándo y dentro de que límites son públicos los asuntos de la vida personal, así como controlar que sucede con sus datos personales. Con esto se logra el libre desarrollo de la personalidad en una sociedad libre, en la cual se presume la protección de las personas frente al tratamiento de sus datos personales[21].

[19] Centro de Investigación y Seguridad Nacional CISEN, disponible en *http://www.cisen.gob.mx/snSegNal.html*
[20] Ponce Baéz, Gabriela y García Tinajero, Leonel, *Las Fronteras del Derecho a la Información*, México, Novum, 2011, p. 70
[21] Remolina Angarita, Nelson, op. cit., p. 29

También podemos señalar que se trata de un derecho fundamental ligado al ser humano en cuando a su dignidad humana, el cual se caracteriza principalmente por proteger del conocimiento ajeno aspectos de nuestra vida personal y familiar.

La idea de la autodeterminación significa decidir por sí mismo los límites sobre lo queremos que sea del dominio público, o lo que queremos que sea del conocimiento del responsable en una relación jurídica. No existe una medida sobre qué dato es más o menos íntimo, tampoco si es sensible o no lo es, todo radica en la utilidad y posibilidad de su aplicación[22].

El tratamiento de la información personal no debería afectar nuestra información intima, para ello existe el derecho a la intimidad[23].

b) Vigilancia y Datos Personales

Con el tratamiento de los datos personales, existe la posibilidad de una vigilancia en la vida cotidiana de los individuos, cuando se obtiene el registro de varios datos que parecieran sin importancia, pero una vez que se relacionan permiten la obtención de un perfil de la persona.

Cuando se obtiene el perfil de una persona se puede saber determinadas características como son estilos de vida, lugares que se visitan, hábitos de consumo y comportamientos, todo implica un tratamiento informatizado de sus datos que pueden suponer una valoración favorable o desfavorable que supondría una discriminación para la obtención de un crédito, un empleo, o en algunos casos ser objeto de una “especial vigilancia y control” cuando se trate de un perfil delincuente o terrorista o simplemente disidente de la ideología mayoritaria.

[22] Garriga Domínguez, Ana, op. cit., p. 32
[23] Ibidem, p. 24

Estas consecuencias son claramente evidentes cuando se relaciona una persona con hechos o situaciones donde su identidad se incorpora por ejemplo a las llamadas listas negras[24].

Consideramos que el derecho a la protección de datos personales a través de la autodeterminación informativa, garantiza a las personas el poder sobre el uso de sus datos personales, así nosotros decidimos en qué medida afecta nuestra privacidad.

Todos estamos de acuerdo que una sociedad debe permitir el libre desarrollo de las personas y contribuir en el entorno público y que se desenvuelven. Una forma de evitar el desarrollo es la existencia de un control absoluto sobre sus datos personales, por medio de herramientas que permiten la creación de perfiles que permiten saber nuestra forma de ser, valores, preferencias políticas, religiosas, sexuales, es decir nuestros datos sensibles[25].

2. Libertad de expresión

Uno de los conceptos de derechos humanos señala que son las prerrogativas sustentadas en la dignidad humana, cuya realización efectiva resulta indispensable para el desarrollo integral de la persona. Este conjunto de prerrogativas se encuentra establecido dentro del orden jurídico nacional, en nuestra Constitución Política, tratados internacionales y las leyes. Todas las autoridades tienen la obligación de respetar y proteger nuestros derechos[26].

Es importante hablar de la libertad de expresión, uno de los derechos fundamentales del hombre, es la prolongación de nuestra garantía individual a pensar, sin la cual no es posible el desarrollo en la sociedad. Históricamente la lucha por la libertad de

[24] Garriga Domínguez, Ana, op. cit., p. 28
[25] Gómez-Robledo y Ornelas Núñez, op. cit., p. 11.
[26] Comisión Nacional de Derechos Humanos. Disponible en http://www.cndh.org.mx/Que_son_ Derechos_Humanos

expresión ha sido una larga batalla contra el autoritarismo y contra el cambio y la innovación[27].

Sin duda es una pieza fundamental en la creación de un sistema político, su regulación, la relación con el Estado, los medios de comunicación y las personas, dan a conocer la existencia o no de un progreso social y el sistema de valores de una nación[28]. La consolidación de la libertad de expresión es el resultado del desarrollo educativo del hombre[29].

Para el autor Ernesto Villanueva, la libertad de pensamiento y expresión es la piedra angular de cualquier sociedad democrática. Nuestro sistema interamericano de derechos humanos, señala un sentido amplio; el artículo 13 de la Convención Americana garantiza el derecho de toda persona a la libertad de expresión, y precisa que este derecho comprende, "la libertad de buscar, recibir y difundir información e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección"[30].

3. Libertad de Expresión en Internet: principios orientadores

Del desarrollo de las tecnologías, considera que el uso de internet ha permitido comunicarse en forma instantánea a bajo costo, pero sobre todo ha cambiado la forma en que compartimos y accedemos a la información. La Corte Interamericana de Derechos Humanos en lo sucesivo la CIDH, considera que las políticas públicas y las regulaciones del Internet deben adecuarse a principios orientadores que informan la labor del Estado.

---

[27] Villanueva, Ernesto, *Régimen jurídico de las libertades de expresión e información en México*, México, Instituto de Investigaciones Jurídicas UNAM, 1998, p. 23
[28] Muñoz Díaz, Pablo Francisco, *Libertad de Expresión: Límites y Restricciones*, México, Escuela Libre de Derecho, 2016, p. 25
[29] Villanueva, Ernesto, *Régimen jurídico de las libertades de expresión e información en México*, México, op. cit., p. 25
[30] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Libertad de Expresión e Internet,* op. cit. p. 1

La CIDH en su informe sobre la libertad de expresión señala los siguientes principios:

1. Acceso: Se refiere a la necesidad de garantizar la conectividad y el acceso universal, ubicuo, equitativo, verdaderamente asequible y de calidad adecuada, a la infraestructura de Internet y a los servicios de las TIC.
2. Pluralismo: Maximizar el número y la diversidad de voces que puedan participar de la deliberación pública es al mismo tiempo condición y finalidad esencial del proceso democrático.
3. No discriminación: Es la obligación del Estado de quitar los obstáculos que impidan a los ciudadanos o un sector difundir opiniones o informaciones.
4. Privacidad: De acuerdo al artículo 11 de la Convención Americana de Derechos Humanos establece "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación", y que "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".
5. Neutralidad de la Red: Es el principio a través del cual el tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación. [31]

Sobre el principio de privacidad se obliga originalmente a los Estados a abstenerse de realizar intromisiones arbitrarias, en su información personal y comunicaciones, asimismo garantizar que otros se abstengan de realizar conductas abusivas.

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA (en lo sucesivo la Relatoría) subraya la importancia en comunicar que la intervención o violación a las comunicaciones tiene

[31] *Cfr*. Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Libertad de Expresión e Internet,* op. cit. p. 7-12

un efecto inhibitorio y que se afecta el pleno ejercicio del derecho a comunicarse, las prácticas de vigilancia, intercepción y recopilación, no solamente afectan el derecho a la privacidad y la libertad de expresión sino que son contrarios a la integración de una sociedad democrática[32].

Es por ello que tomamos en consideración que la recopilación y conservación de datos como lo hacen en México, encuadra perfectamente en una conducta que no solo afecta el derecho a la privacidad, también la libertad de expresión con el control y uso indiscriminado por parte de la autoridad.

4. Limitaciones a la libertad de expresión

De acuerdo a la Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, se han realizado una serie de recomendaciones o principios en los temas de terrorismo y seguridad nacional, por lo general la autoridad utiliza ese término de seguridad para justificar las violaciones a las privacidad, sin embargo las acciones que realiza el Estado, como es el caso de México con la supuesta “Cooperación Judicial” en materia de telecomunicaciones en donde se autoriza el uso de la conservación de datos de telecomunicaciones es evidente que pueden afectar la libertad de pensamiento, libertad de expresión y el derecho a la intimidad de las personas.

A continuación, señalamos las recomendaciones que consideramos relevantes para la debida conservación de datos personales y que deben de servir de base para la implementación y uso del programa de cooperación judicial al cual están obligados los concesionarios telecomunicaciones en la conservación de datos.

En la **tercera** recomendación, se acepta y reconoce que cuando sea necesario por cuestiones de protección en los supuestos de seguridad nacional es justificable el uso de forma excepcional de la vigilancia de las comunicaciones privadas, pero no

[32] Ibidem, p. 9

debemos olvidar que este tipo de vigilancia constituye un acto invasivo a la privacidad, la libertad de pensamiento y libertad de expresión[33].

En la **cuarta** recomendación se menciona la importancia del uso de Internet y como ha creado oportunidades para la libertad de expresión, comunicación, búsqueda, posesión e intercambio de información. Con ello se ha facilitado el intercambio de datos que incluyen su localización, saber con quienes se comunican, actividades, con toda esa información contenida en bases de datos en forma accesible y sistematizable, tiene como consecuencia que en su conjunto puede ser altamente reveladora, es por ello que los programas en contra del terrorismo y la seguridad nacional, se ha generalizado sin la debida regulación.[34]

Y consideramos que México no es la excepción ha adoptado una medida completamente violatoria de derechos humanos, tal vez basada en una justificación de seguridad, pero hasta qué punto es viable vigilar y recopilar la información que se transmite en las telecomunicaciones, y debemos preguntarnos porque los concesionarios han permitido la aplicación de la Ley Federal de Telecomunicaciones y Radiodifusión.

Como **quinta** recomendación tenemos que la legislación en materia de inteligencia y seguridad es insuficiente frente a las nuevas tecnologías de la información. Pero sobre todo, es preocupante el efecto intimidatorio derivado del acceso indiscriminado a los datos porque puede afectar a la libertad de expresión, pensamiento, búsqueda y difusión de información de las personas.[35]

En la **sexta** recomendación, se reconoce la necesidad que los Estados establezcan límites a la potestad para vigilar las comunicaciones privadas, de acuerdo con la

[33] *Cfr.* Relator Especial de la Naciones Unidas (ONU), *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*, op. cit. Punto 3
[34] Ibidem, punto 4
[35] Ibidem, punto 5

proporcionalidad y respetando los derechos de las personales y los principios de derecho internacional.[36]

Como se expone en esta Declaración, los derechos a la privacidad y a la libre circulación del pensamiento e información se encuentran protegidos por el derecho internacional de derechos humanos. Se prohíben injerencias arbitrarias o abusivas en la vida privada, incluidas las comunicaciones y a obtener protección del Estado en contra de este tipo de injerencias.

En el **octavo** punto, para que el Estado garantice la intervención y recolección y uso de la información personal, deberá incluir las limitaciones de la persona afectada a acceder a esa información, lo cual deberá estar claramente autorizadas por ley. La ley deberá establecer:

a) Límites respecto a la naturaleza, alcance y duración de las medidas
b) Las razones para ordenar las medidas
c) Las autoridades competentes para autorizar, ejecutar y supervisarlas
d) Los mecanismos legales para su impugnación[37].

De acuerdo con nuestro tema, la **novena** recomendación en la Declaración conjunta, se menciona que la ley debe autorizar el acceso a las comunicaciones y a datos personales sólo en las circunstancias excepcionales definidas en la legislación. Cuando se alegue la seguridad nacional deben especificarse los criterios, es decir únicamente cuando existe un riesgo cierto y cuando ese daño seas superior al interés general de mantener el derecho a la privacidad. Asimismo, se habla de la creación de un organismo de control independiente que monitoree la entrega de la información[38].

[36] Ibidem, punto 6
[37] Ibidem, punto 8
[38] Ibidem, punto 9

En el **décimo** punto se recomienda que la vigilancia de las comunicaciones y las injerencias a la privacidad no deben exceder a lo señalado en la normativa y que las finalidades para la cual se entrega la información no sea usada para cuestiones distintas, por lo que debe implementar sanciones severas para quienes obtengan información de forma clandestina. Aquí se incluye la información obtenida por motivos políticos contra periodistas y medios de comunicación.[39]

Los concesionarios o empresas de servicios de comunicaciones deberán asegurarse de que se respeten los derechos a la protección de datos de sus clientes y de usar internet sin injerencias arbitrarias de acuerdo a lo manifestado en el punto once de la Declaración conjunta.

Otra recomendación en cuanto al tema de transparencia se encuentra en el número **doce**, aquí se señala la obligación por parte de los Estados de difundir al menos lo siguiente:

a) El marco regulatorio de los programas de vigilancia;
b) Los órganos encargados para implementar y supervisar los programas;
c) Los procedimientos de autorización;
d) Selección de objetivos y manejo de datos;
e) Así como la Información sobre el uso de las técnicas sobre el manejo de datos.[40]

En todos los supuestos se debe garantizar la transparencia y rendición sobre el uso e implementación de los programas.

En el punto **trece**, se establece al Estado que permita a los concesionarios informar a los clientes sobre los procedimientos a las solicitudes de vigilancia y deberán

[39] Ibidem, punto 10
[40] Ibidem, punto 12

informar el número y el alcance de las solicitudes que reciban dichos concesionarios.[41]

A la entrada en vigor de la LFTR, los concesionarios tenían la obligación de comunicarnos los cambios en el tratamiento de nuestros datos personales, así tenemos que no corresponden las finalidades del tratamiento con las transferencias que se realizan, por lo menos los concesionarios debieron cumplir con la obligación de informarnos que realizaran transferencias a las autoridades judiciales mediante un requerimiento de la autoridad competente.

Otra recomendación es divulgar la información sobre programas ilegales de vigilancia de comunicaciones privadas, los Estados deben identificar y sancionar a quienes realicen vigilancia e informes a las presuntas víctimas, de acuerdo lo mencionado en dicha recomendación.

En el punto **quince** bajo ninguna circunstancia, los periodistas, integrantes de los medios u organizaciones de la sociedad civil que difundan información sobre programas de vigilancia por ser de interés público puedan ser sometidos a sanciones ulteriores. Las fuentes confidenciales relacionadas con la divulgación de información deben ser protegidas por la ley.[42]

En la recomendación **dieciséis**, debe respetarse el supuesto que una persona qué aun teniendo la obligación de mantener confidencialidad de información con el Estado, divulgue información que sea considerada violaciones a derechos humanos no debe ser objeto de sanción.[43]

[41] Ibidem, punto13
[42] Ibídem, punto 15
[43] Ibidem, punto 16

Por último, en la recomendación **diecisiete** se establecen reglas para la imposición de sanciones a quienes revelan información reservada, mediante leyes previamente establecidas y garantizando el debido proceso.[44]

Como vemos todas estas recomendaciones debieron tomarse en consideración al momento de establecer la normativa que regula la recopilación, conservación y entrega de la información de las comunicaciones.

5. Derecho a la Privacidad

Para definir lo privado debemos tomar en consideración los medios jurídicos para protegerlo, los cuales van a variar de acuerdo al tiempo y lugar, así como del tipo de gobierno y desarrollo de cada país[45].

De acuerdo a la definición del autor Ernesto Villanueva, define el derecho a la vida privada de la siguiente forma:

> "… consiste en la prerrogativa que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público". El bien jurídicamente protegido de este derecho está constituido por la necesidad social de asegurar la tranquilidad y la dignidad necesarias para el libre desarrollo de la personalidad humana…[46].

Es decir, todo aquello que nosotros no deseamos que sea del conocimiento de los demás, nosotros ponemos el límite a esta privacidad.

---

[44] Ibidem, punto 17
[45] Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (Infodf), *Retos de la protección de datos personales en el sector público,* México, Infodf, 2011, p. 434
[46] Villanueva, Ernesto, *Derecho de acceso a la información pública en Latinoamérica*, México, UNAM, 2003, p. LXXIV.

Como seres humanos podemos elegir lo que queremos sea público y que no, lo cual no debe ser de interés de la autoridad y si en todo momento tuviéramos la obligación de hacer del conocimiento a la autoridad lo que hacemos o el deber de obedecer a otros, se perdería esa condición humana, es esencial la existencia de límites al Estado para evitar un abuso en el uso de sus facultades[47].

La protección a la vida privada es un derecho reconocido por diversas disposiciones internacionales de la cuales México forma parte, entre las que se encuentra la propia Convención Americana sobre los Derechos Humanos, que dispone: "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra y reputación.

La CPEUM, señala el derecho a la vida privada como límite a la intromisión del Estado en el ámbito de la persona, por ello el artículo 16 establece que "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento"[48].

Por su parte la Suprema Corte de Justicia de la Nación (en lo subsecuente la SCJN), ha determinado que la garantía de seguridad jurídica de todo gobernado a ser molestado sino mediante mandato emitido por la autoridad competente, fundado y motivado, tiene la finalidad primordial de proteger la vida privada personal y familia.[49]

---

[47] Escalante Gonzalbo, Fernando, *"El Derecho a la privacidad"*, México, Instituto Federal de Acceso a la Información y Protección de Datos, Cuadernos de Transparencia, Número 2, 9ª reimpresión 2012, p. 8

[48] Gómez-Robledo y Ornelas Núñez, *op. cit.*, pp. 13-14.

[49] **DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.**
Dicho numeral establece, en general, la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado, de lo que deriva la inviolabilidad del domicilio, cuya finalidad primordial es el respeto a un ámbito de la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la Constitución Política de los Estados Unidos Mexicanos establece para las autoridades. En un sentido

En el artículo 6 de la CPEUM, se regula el derecho a la libertad de expresión estableciendo entre sus límites la privacidad, y en el artículo 16, describe los elementos comprendidos por el Derecho a la privacidad:

> **Artículo 6o.** La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida **privada** o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.
>
> […]
>
> **A.** Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> […]
>
> **II.** La información que se refiere a la vida **privada** y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
>
> […]

Por ello el concepto de vida privada es muy extensa y genérica, porque se refiere a todo aquello que no queremos que sea del conocimiento de la sociedad sobre una particularidad. En la vida privada existe a su vez información que por lo general deseamos proteger por considerar como esencia de la persona, y que se conoce como el concepto de intimidad[50].

Como fue señalado, la definición legal de lo privado, se establece de acuerdo a la cantidad de recursos para protegerlo, y depende de las ideas que en su momento se utilicen porque cambian con el tiempo, también cambia con el avance de la tecnología con la que se puede vigilar, interferir o asegurar cada ámbito.

---

amplio, la referida garantía puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en el artículo 16, primer párrafo, constitucional, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida. Tesis 2a. LXIII/2008, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXVII, mayo de 2008, p. 229

[50] Gómez-Robledo y Ornelas Núñez, op. cit., p. 6.

Actualmente, respecto a las telecomunicaciones se tiene que legislar con respecto al uso de la informática la cual ha evolucionado la velocidad y la cantidad de información que se puede compartir o difundir[51].

Principalmente lo privado, implica la protección ante los demás, en los asuntos privados tenemos no solo el derecho a decidir, también a guardar secreto sobre nuestros actos, por eso nadie podría decir libremente si nos encontráramos expuestos a discriminaciones, reproches o censura ante los demás. Las formas de presión como la burla, la humillación puede ser ultrajantes para la dignidad[52].

Con el derecho a la privacidad el bien jurídico tutelado es la tranquilidad y dignidad de las personas, esto les permite que puedan desarrollar libremente su personalidad[53].

El derecho a la privacidad dicho de otra forma se realiza cuando se protegen informaciones de las personas y que tratamos de mantener fuera del conocimiento de terceros como son las cuestiones laborales, los expedientes médicos, legales y personales, la convivencia familiar, la correspondencia, la intimidad sexual, entre otros.

Por último, se consideraba el derecho a la vida privada de las personas, como una limitante al derecho a la información, pero la información personal puede ser clasificada como confidencial, sin embargo, nos encontramos frente a dos derechos humanos que persiguen fines diferentes sin que uno signifique una limitación del otro[54].

---

[51] Escalante Gonzalbo, Fernando, op. cit., p. 9
[52] Ibidem, p. 9
[53] Mirón Reyes, Jorge Antonio, *Ataques a la vida privada y a la intimidad frente al derecho de acceso a la información*, Instituto de Investigaciones Jurídicas, disponible en: http://historico.juridicas. unam.mx/publica/rev/decoin/cont/8/ art/art3.htm#N1
[54] Villanueva, Ernesto, *Seguridad nacional, información y poder legislativo,* op. cit, p. 196

6. Privacidad de las Comunicaciones

El respeto a la libertad de expresión también engloba la privacidad de las comunicaciones, de acuerdo a lo señalado en el artículo 11 de la Convención Americana sobre Derechos Humanos y de acuerdo a la jurisprudencia interamericana el objeto de la privacidad es garantizar que las personas disfruten de un ámbito reservado de su vida sin la intervención, conocimiento o la divulgación del Estado o de terceros.

El derecho a la privacidad protege al menos cuatro bienes jurídicos, que se relacionan con el ejercicio de otros derechos fundamentales como la libertad de pensamiento y expresión.

a) En primer lugar, el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas.
b) En segundo lugar, el derecho a gobernarse, en ese espacio de soledad, por reglas propias definidas de manera autónoma según el proyecto individual de vida de cada uno.
c) En tercer lugar, el derecho a la vida privada protege el secreto de todos los datos que se produzcan en ese espacio reservado, es decir, prohíbe la divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona.
d) Y, finalmente, la protección de la vida privada protege el derecho a la propia imagen, es decir, el derecho a que la imagen no sea utilizada sin el consentimiento del titular[55].

Con el uso de los medios digitales y las redes sociales se ve una clara colisión de forma constante con el derecho a la vida privada y la concepción de privacidad. Es

[55] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Libertad de Expresión e Internet,* op. cit. pp. 62 y 63

evidente que los proveedores de servicios de aplicaciones como son las redes sociales incumplen sus obligaciones como responsables en donde permite que las personas sean contactadas por cualquier persona y no solo por sus contactos, incluso los usuarios comparten su vida privada como son fotografías, lugares que visitan, en términos generales una gran cantidad de información personal.

En estos momentos la privacidad no es algo que se crea por cada persona, por que intervienen otras personas, si tenemos conciencia que otros respeten nuestra privacidad nos están protegiendo. Dependerá de nosotros mismos el cuidado de la identidad propia o ajena, asimismo la educación y la creación de una cultura sobre la protección de los datos personales, generará la exigencia hacía los proveedores de servicios en su carácter de responsables del cumplimiento de sus obligaciones[56].

[56] Comisión para el Acceso a la Información Pública y Protección de Datos et. al, *Transparentemente: Protección de Datos Personales*, Privacidad en las Redes sociales, Vicuña de Nicolás, Iñaki., México, Comisión para el Acceso a la Información Pública y Protección de Datos (Puebla), 2012, p.70

CAPÍTULO SEGUNDO. DISPOSICIONES LEGALES EN MATERIA DE CONSERVACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

1. Ley Federal de Telecomunicaciones y Radiodifusión

Los medios electrónicos ahora son los medios de comunicación masiva y los concesionarios están obligados a respetar el interés público del servicio que prestan.[57] Los concesionarios de telecomunicaciones y radiodifusión deben someterse a los límites que marca la Constitución, y deben asumirse como empresas que cumplen una función social[58].

Con la entrada en vigor el 14 de agosto de 2014 de la Ley Federal de Telecomunicaciones y Radiodifusión (en lo sucesivo la LFTR), las empresas de telecomunicaciones se encuentran obligadas a conservar una gran cantidad de datos conocidos como “metadatos de comunicaciones” de todos sus usuarios. Esta obligación establece el plazo de conservación de los datos personales por 12 y el plazo a 24 meses.

Como ya lo hemos señalado tenemos que exigir nuestros derechos como usuarios de las telecomunicaciones para exigir el exigir el cumplimiento y respeto por parte del Estado, el sector privado y la sociedad en general[59].

La Constitución dispone derechos fundamentales relacionados con las telecomunicaciones, como son el derecho fundamental de acceso a las tecnologías de la comunicaciones incluyendo radio, televisión abierta, internet y banda ancha, permitir la libre circulación de ideas y de no injerencia, el carácter de las telecomunicaciones y la radiodifusión como servicios públicos con ciertas características, y la no intervención de comunicaciones privadas, salvo en los términos y condiciones previstos expresamente en la Constitución y en las leyes[60].

---

[57] Asociación Mexicana de Derecho a la Información (AMEDI), *Panorama de la comunicación en México 2011: Desafíos para la calidad y diversidad,* México, Gráficos eFe, 2011, p. 13
[58] Ibidem, p. 20
[59] Álvarez, Clara Luz, *Derechos de los usuarios de telecomunicaciones*, México, Instituto de Investigaciones Jurídicas UNAM, 2006, p. 3
[60] Ibidem, p. 4 y 5

2. Posicionamiento sobre la inconstitucionalidad del artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión.

A la entrada en vigor de la LFTR, el INAI realizo su posicionamiento sobre la posibilidad de presentar una acción de inconstitucionalidad, considero importante hacer este señalamiento, que sirve como sustento para considerar viable el establecimiento de límites a la conservación de datos.

De algunas posturas de los Comisionados del INAI podemos reafirmar que la conservación de datos es inconstitucional sobre todo por la falta de proporcionalidad en la medida que afecta a la privacidad.

Como lo hemos señalado de acuerdo al párrafo primero del artículo 16 de la CPEUM, nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de un mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

El artículo 190 de la LFTR establece los siguiente:

> **Artículo 190.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:
>
> […]
>
> **II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad**, que permitan identificar con precisión los siguientes datos:
>
> **a)** Nombre, denominación o razón social y domicilio del suscriptor;
>
> **b)** Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);
>
> **c)** Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;
>
> **d)** Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

Para tales efectos, el concesionario deberá **conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes**, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos **por doce meses adicionales en sistemas de almacenamiento electrónico**, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

[…]

(***Énfasis añadido)***

Derivado de lo anterior, en su momento el INAI, realizó un *posicionamiento sobre la inconstitucionalidad del artículo 190* de la LFTR, en la cual decidieron no interponer una acción de inconstitucionalidad, por ello hacemos mención sobre el organismo autónomo encargado de la protección personales en nuestro país, sobre las violaciones a derechos humanos y la privacidad.

Un punto principal en nuestro trabajo, con el multicitado artículo *190 fracción II que ordena la retención de datos*, como son origen de las llamadas, duración, ubicación, mensajes de texto, actividad en la red—de 12 hasta por 24 meses y la creación de una base de datos por parte de los concesionarios de telecomunicaciones para que autoridades, puedan acceder a ellos sin orden judicial.

Por ello consideramos que la retención, conservación y recopilación de datos personales, se lleva a cabo de manera indiscriminada, no es correcto que se realice a todos los usuarios sin que exista un indicio, supuesto o se presuma una circunstancia que justifique la violación a la privacidad.

Ahora bien, de acuerdo al análisis se hace mención de lo que consideramos relevante dentro de los posicionamientos de algunos comisionados.

a) Comisionada Areli Cano Guadiana

Para la Comisionada Areli Cano Guadiana, la LFTR no establece en forma clara y precisa cuales son las autoridades competentes, ni la materia o los delitos por los cuales se podrán formular las solicitudes correspondientes de información[61]. El artículo 189 de la LFTR, establece de manera genérica que los concesionarios de telecomunicaciones, los autorizados y proveedores de servicios están obligados a atender todo mandamiento por escrito, fundado y motivado de la "autoridad competente" en los términos que establezcan las leyes, sin precisar quién es la autoridad competente, lo cual desde luego transgrede el derecho fundamental de seguridad jurídica, ya que las personas no tienen posibilidad de conocer cuál es la autoridad facultada para solicitar este tipo de información, además que deja abierta la posibilidad para que surjan abusos por parte de las autoridades investigadoras[62].

[61] INAI. *Posicionamiento de los Comisionados del IFAI, sobre la inconstitucionalidad de los artículos 30, 189 y 190, fracciones I, II y III de la Ley Federal de Telecomunicaciones y Radiodifusión.* Disponible en http://inicio.ifai.org.mx/nuevo/Posicionamientos%20de%20los%20Comisionados%20del%20IFAI.pdf, p. 3
[62] Idem

Coincidimos con este planteamiento no debe dejarse a la interpretación cual es la autoridad competente, pues varias autoridades pueden adecuarse a “instancias de seguridad” o mal interpretar la Ley de Seguridad Nacional y la Ley General del Sistema Nacional de Seguridad Pública.

Respecto a la fracción II del artículo 190 de la LFTR, contempla la obligación de los concesionarios de telecomunicaciones de conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea a contarse a partir de la fecha en que se haya producido la comunicación[63].

Como vemos el plazo de conservación no justifica, las personas no están sujetas a un procedimiento como presuntos responsables por la comisión de un delito, pero sin motivo se usa en forma general, esta disposición afecta a los millones de usuarios de la población mexicana, porque no establece limitaciones geográficas o casos de excepción, lo cual implica una violación al principio de presunción de inocencia consagrado por el artículo 20, apartado B), fracción de la Constitución Política de los Estados Unidos Mexicanos.

Con esta disposición no se protege a los ciudadanos y se desvía del objetivo principal que es la seguridad, por el contrario, con la obtención de estos datos las autoridades básicamente realizan una labor de vigilancia durante el período de conservación, esto afecta la privacidad de los titulares de las líneas telefónicas. También se debe tomar en consideración que no se garantiza ni se precisa los métodos de eliminación de la información.

Por último la Comisionada señala que en relación al artículo 190, fracción III de la LFTR, no prevé criterios objetivos para la transmisión y custodia de la información proporcionada; la cantidad y tipo de datos personales que deben aportar los concesionarios de telecomunicaciones, a las autoridades competentes; no

[63] Ibidem, pp. 11 y 12

establece algún parámetro objetivo que permita limitar el número de servidores públicos de las instancias de seguridad o de procuración de justicia que tendrán acceso a los datos conservados.

b) Oscar Mauricio Guerra Ford

El derecho a la protección de datos personales está regulado en los artículos 6, inciso A, fracción II y 16, segundo párrafo de la Constitución. Por una parte garantiza el poder de disposición que las personas tienen respecto de su información personal para lograr un adecuado desarrollo de su personalidad y, por otra parte, obliga a los responsables (sujetos obligados) o particulares a que traten los datos personales conforme a lo dispuesto en las Leyes.

Es fundamental en la protección de los datos personales la autodeterminación de la información el cual supone que los titulares de los datos pueden decidir qué información de la esfera privada puede ser conocida o cuál debe permanecer en secreto, así como elegir quién y bajo qué condiciones puede utilizar esa información[64].

El artículo 190, fracción II, de la LFTR, expedida mediante decreto publicado en el Diario Oficial de la Federación el día 14 de julio de 2014, establece de manera precisa la obligación de los concesionarios de tratar y conservar diversos datos de carácter personal, asociados a los titulares de las líneas telefónicas, por ello coincidimos con su criterio en donde claramente se **vincula al aparato telefónico con el titular de la línea telefónica,** con la adición de otros datos de las comunicaciones que éste realice.

Estamos de acuerdo en que dicha normativa conlleva el tratamiento de datos personales de los titulares de las líneas telefónicas, y en consecuencia debería

[64] Ibidem, pp. 25 y 26

sujetarse el tratamiento a lo dispuesto en los artículos 6 y 16 constitucionales, y las leyes especiales en materia de protección de datos personales[65].

De acuerdo a lo anterior el tratamiento de datos personales se realiza sin el consentimiento de los usuarios y sin la debida información por ello se vulnera el derecho a la protección de los datos personales consagrado en el artículo 16 constitucional, porque afectan el derecho a la autodeterminación.

Se reitera la afectación debido a que no se establece de manera clara y precisa que autoridades pueden tener acceso a los datos conservados, no establece excepciones y no indica procedimiento para la eliminación de los datos y las medidas contra el abuso, por lo tanto, no se cumple con el requisito de necesidad y proporcionalidad.

Otro punto importante en el periodo, no es correcto establecer un periodo de conservación obligatorio de 2 años, porque no da la posibilidad al titular de los datos de ejercer su derecho de cancelación y oposición, y de acuerdo a la LFPDPPP, se pueden ejercer en cualquier momento.

La conservación de datos consagrada en el artículo 190 fracciones II y III de la LFTR, constituye también una interferencia con el derecho a la inviolabilidad de las comunicaciones.

Con la aplicación de los artículos 189, 190 fracciones I, II y III se expondría a todos los usuarios de una línea telefónica al riesgo de que las autoridades investiguen sus datos, conozcan su contenido, se informe sobre su vida privada y utilicen esos datos para múltiples fines, teniendo en cuenta, en particular, el inconmensurable número de personas que tienen acceso a los datos durante un período mínimo de doce o veinticuatro meses de conservación[66].

[65] Ibidem, p. 26
[66] Idem

Es rescatable la opinión del Comisionado Guerra Ford, por su preocupación en el cumplimiento de la LFPDPPP, así mismo considero necesario tomar en cuenta la doctrina internacional para pronunciarse a fondo sobre el problema planteado.

3. Lineamientos de Colaboración en Materia de Seguridad y Justicia

En fecha 2 de diciembre de 2015, el Instituto Federal de Telecomunicaciones (en lo sucesivo el IFT) publicó en el Diario Oficial de la Federación, los **Lineamientos de Colaboración en Materia de Seguridad y Justicia**, en los que se menciona las reglas para el cumplimiento de las solicitudes de acceso al registro de comunicaciones y de localización geográfica en tiempo real de equipos de comunicación móvil.

De acuerdo con el considerando segundo, es obligación del Estado Mexicano garantizar la **seguridad pública, la seguridad nacional**, así como una efectiva procuración de justicia, por lo que en la LFTR se incluyó el Título Octavo "De la Colaboración con la Justicia", que establece la obligación de los Concesionarios de telecomunicaciones y Autorizados de atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes.

De acuerdo al quinto considerando, se menciona con la transformación de las tecnologías de la información y comunicación, la telefonía móvil y el Internet son servicios de mayor penetración a nivel mundial, imprescindibles para todas las actividades de la sociedad.

En el punto 3 del considerando quinto, se menciona el incremento de la inseguridad entre 2006 y 2011, no sólo se cometieron más delitos además fueron con mayor violencia. El costo total estimado por la inseguridad y el delito en 2014 alcanzó 226

mil 700 millones de pesos, lo que representó 1.27% del PIB según la Encuesta Nacional de Victimización y Percepción Sobre seguridad Pública (INEGI, 2015).

De acuerdo al alto índice delictivo, la inseguridad se vuelve un tema prioritario y la principal preocupación de la ciudadanía, incluso por encima del desempleo y la pobreza. Por ello es necesario la generación de inteligencia para la seguridad pública, la información para la toma de entre las instituciones, por ello el uso de las tecnologías de la información y comunicación es una herramienta indispensable, las Procuradurías de Justicia Estatales[67], manifestaron en el caso de delitos cometidos mediante la utilización de servicios de telecomunicaciones, *los datos relativos a las comunicaciones efectuadas son indispensables para la investigación y persecución del delito.*

Las procuradurías estatales, señalan que el registro, conservación control de los datos, son un elemento importante para averiguar, y sirve para conocer la ruta de una comunicación, a fin de prevenir, investigar y/o combatir delitos. Asimismo, señalan un alto porcentaje de delitos llevados a cabo mediante dispositivos o Equipos Terminales Móviles, ahí la importancia de contar con información relacionada con el equipo que les permitan iniciar líneas de investigación.

En el punto 4 del Considerando Quinto se menciona que ha petición del entonces Instituto Federal de Acceso a la Información y Protección de Datos, se debe respetar el marco normativo de las comunicaciones privadas y la prohibición de utilizar los datos conservados para fines distintos a los previstos y que cualquier uso distinto será sancionado por las autoridades.

Por ello los Lineamientos establecen las características que deben tener los sistemas de los Concesionarios y Autorizados a fin de garantizar la integridad y seguridad de la información transmitida, manejada y resguardada, basada en

[67] XXXIII Asamblea Plenaria de la Conferencia Nacional de Procuración de Justicia.

estándares internacionales respecto a la protección de los Datos Personales de los usuarios, así como para la cancelación y supresión segura de la información.

De acuerdo a los Lineamientos los concesionarios, autorizados y proveedores de servicios y aplicaciones están obligados a atender todo mandamiento por escrito fundado y motivado. Así como la obligación en caso no contar con la infraestructura para el cumplimiento de los lineamientos están obligados a contratar a concesionarios que cuenten con los servicios.

En su artículo décimo segundo, se establece que las comunicaciones privadas son inviolables y solo la autoridad judicial federal podrá autorizar la intervención de cualquier comunicación privada a petición de la autoridad federal o el Ministerio Público de la entidad federativa.

De acuerdo al artículo décimo tercero, los concesionarios deben enviar el número que identifique el origen de la llamada sin alteraciones que impidan identificarlo.

Los concesionarios de telecomunicaciones tienen la obligación de contar con la capacidad de almacenar y entregar los datos, el artículo décimo cuarto se señala lo siguiente:

> Para el caso de líneas privadas se conservarán el nombre del usuario registrado, la dirección de origen y destino de la línea;
> Para el caso líneas fijas se registrará y conservará la información correspondiente a:
>
> > Nombre y dirección del usuario registrado;
> > Tipo de Comunicación;
> > Números de origen y destino, y
> > Duración, fecha y hora de la comunicación.
>
> Para el servicio móvil en las modalidades de prepago y pospago se registrará y conservará la información correspondiente a:

Nombre y dirección del usuario registrado, en el caso de la modalidad de pospago;

Tipo de Comunicación;

Los números de origen y destino;

Duración, fecha y hora de la comunicación;

Fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda);

La etiqueta de localización (identificador de celda);

IMEI;

IMSI;

En su caso, los IMSIs asociados a un mismo IMEI;

Modalidad de pago, y

En su caso, características técnicas del Dispositivo o Equipo Terminal Móvil.

En el caso de la modalidad de prepago, se registrarán y conservarán además los datos que permitan identificar:

El lugar, fecha y hora en la que se realizó la compra del dispositivo de prepago y/o la tarjeta SIM, en el caso en que el Concesionario o Autorizado los comercialice por canales propios, o

En su caso, los datos del distribuidor al que fue entregado el dispositivo de prepago o la tarjeta SIM para su comercialización.

En el artículo décimo séptimo señala que los concesionarios de telecomunicaciones son responsables respecto a la posesión, tratamiento y control de los datos personales de los particulares.

Existe la obligación de un informe semestral que se deberá entregar en enero y julio de cada año, el cual deberá contener, el número total de requerimientos por autoridad facultada, desglosando las recibidas, entregadas y no entregadas mensualmente.

La información estadística de los informes semestrales debe ser publicada en el portal de internet del IFETEL, conforme a las obligaciones de transparencia. En caso de que exista una vulneración al tratamiento de los datos personales los concesionarios deberán notificar en forma inmediata a los titulares o usuarios y deberán señalar que medidas se pueden adoptar para disminuir o evitar cualquier afectación.

De acuerdo a lo anterior, es importante resaltar la obligación de las empresas concesionarias y autorizadas a para prestar servicios de telecomunicaciones, de entregar al IFETEL en los meses de enero y julio un informe semestral electrónico.

Asimismo, es muy importante que el IFETEL debe hacer públicos dichos informes en su sitio de Internet.

De acuerdo al artículo sexto transitorio de los Lineamientos del IFT, los informes semestrales deben de empezar a emitirse y solicitarse, respectivamente, a partir de julio de 2016[68].

Vemos que el registro o conservación de datos se realiza en forma generalizada a todas las personas, sin establecer diferencias, limitaciones o excepciones, por lo que afecta a más 101 millones de usuarios de líneas de telefonía celular. Es decir, a todas las personas que utilizan servicios de telefonía móvil en México, sin que los titulares tengan una relación directa o indirectamente a las actividades relacionadas con la procuración de justicia. Con ello se perjudica a todas las personas con la que ni siquiera existe un indicio relacionado con un hecho ilícito. Debe hacerse la valoración sobre si la violación a los derechos humanos está justificada[69].

[68] Red en Defensa de los Derechos Digitales, op. cit., p. 33
[69] INAI, *Posicionamiento de los Comisionados del IFAI,* op. cit, p. 30

4. Ley Federal de Protección de Datos Personales en Posesión de los Particulares

El derecho fundamental a la protección de los datos personales se encuentra regulado en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.

Asimismo, con la expedición de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en lo sucesivo la LFPDPP) el 5 de julio de 2010, se protegen los derechos de los titulares de los datos personales a exigir a los responsables del tratamiento, por ello se deben facilitar los derechos ARCO que son el acceso, rectificación, cancelación y oposición. Se implementan limitaciones para su divulgación publicación o cesión. Y se reconoce los principios que deben utilizarse en el tratamiento de datos personales por parte de todos los entes privados[70].

Actualmente con la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, ya se establecen los mismos principios, limitaciones para transferencias y sanciones en caso de incumplimiento. Con esta ley se homologa la protección de datos para el sector público.

Con la LFPDPPP las personas tienen la protección a través de la autodeterminación, una facultad esencial para elegir que datos puedan ser utilizados y para las finalidades que queremos.

Los principios y deberes se complementan con la acción del titular, conocida como la autodeterminación informativa, entendida como la libertad de decidir qué datos pueden ser utilizados[71].

[70] Luna Pla, Issa, et. al., *Resoluciones relevantes. En materia de acceso a la información y protección de datos personales*, México, INAI, 2016, p. 165
[71] Ibidem, p. 166

Principios de la LFPDPPP

Son las obligaciones que tienen los responsables en el tratamiento de los datos, estos fueron creados antes de la actual era digital en la que vivimos y que ha evolucionado cuando hablamos de las TIC[72]. Para garantizar el derecho a la protección de datos personales y que el titular tenga el control sobre sus datos personales, el tratamiento se debe llevar cabo mediante una serie de principios para que los responsables que utilizan datos en el desarrollo de sus actividades no afecten a los titulares.

Dicho de otra forma, los responsables deben garantizar y disminuir los riesgos en el tratamiento de los datos personales, con el establecimiento de límites se disminuyen los peligros en el tratamiento de datos personales, sin olvidar que se garantiza la idoneidad de la información y la seguridad. Estos límites son conocidos básicamente como principios.

Cualquier responsable debe cumplir con los principios los cuales llevan un orden de valoración para quienes usan, obtienen, almacenan trasmiten, transfieren, manejan, usan los datos personales, ante un conflicto o disparidad con las normas el contenido de los principios prevalece y deberá de observarse aún en contra de la norma técnica de derecho[73].

Ahora bien, todo tratamiento de datos personales debe estar determinado por los siguientes principios:

- **Principio de licitud**

El primero de los principios de datos personales, es decir que los datos personales tienen que ser tratados forma lícita y leal, esto significa utilizar los datos conforme a

[72] Ornelas Nuñez y Alcalde Urbina, op. cit., p. 44.
[73] Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (Infodf), op. cit., p. 199

las leyes. Solo podremos utilizar los datos para aquello que este legalmente permitido, este principio lo encontramos en el artículo 7 de la LFPDPPP.

La obtención de los datos personales no puede realizarse a través de medios engañosos o fraudulentos, por eso no deben recabarse con dolo, mala fe o negligencia; no deben vulnerar la confianza del titular y tratar los datos conforme a lo acordado y que se informe de las finalidades en el aviso de privacidad[74].

Podemos destacar que el responsable tiene las siguientes obligaciones para el principio de licitud:

a) Utilizar los datos conforme al cumplimiento de la legislación mexicana y el derecho internacional.
b) No utilizar medios engañosos o fraudulentos para la obtención de los datos personales, y
c) Respetar la expectativa razonable de privacidad del titular.

Para el caso de los requerimientos de las autoridades a los concesionarios de telecomunicaciones, todo tratamiento de datos personales debe obedecer exclusivamente a atribuciones legales de cada responsable.

- **Principio de consentimiento**

Este principio reconoce que cualquier uso, obtención, recolección y transferencia de datos personales, debe realizarse previo conocimiento y mediante la manifestación de la voluntad del titular de proporcionarlos.

[74] LFPDPP. Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.
La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.
En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.

Es obligación de quienes recogen los datos de obtener el consentimiento de los titulares e informarles del uso y finalidad que tendrá la recolección. El responsable de contar con el consentimiento y la solicitud debe ir siempre ligada a las finalidades concretas las cuales se deben informar en el Aviso de Privacidad.

El consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad.

De conformidad con el artículo 14 segundo párrafo del Reglamento de la LFPDPPP, cuando el responsable no tenga contacto con los titulares previo a la utilización de sus datos personales, pueden ser estos supuestos:

1. Si se obtiene de forma *indirecta*, cuando el titular no los dio personalmente o de manera *directa* al responsable, por ejemplo, mediante una transferencia o los obtuvo de una fuente de acceso público, y
2. Cuando se pone el aviso de privacidad se ponga a disposición por un medio que no es personal o directo, como por ejemplo su envío a través de correo postal.

El responsable deberá informar que el titular cuenta con 5 días hábiles para manifestar su negativa al tratamiento para las finalidades que requieren del consentimiento cuando sea tácito. Porque en el caso de que se requiera expreso y expreso por escrito forzosamente deberá contactar de forma personal o directa la titular[75].

[75] RLFPDPP. Artículo14.
[…]
En los casos en que los datos personales se obtengan de manera indirecta del titular y tenga lugar un cambio de las finalidades que fueron consentidas en la transferencia, el responsable deberá poner a disposición del titular el aviso de privacidad previo al aprovechamiento de los datos personales. Cuando el aviso de privacidad no se haga del conocimiento del titular de manera directa o personal, el titular tendrá un plazo de cinco días para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular. Si el titular no manifiesta

La LFPDPPP en su artículo 10 señala los supuestos de excepción al consentimiento, es decir no será necesario que el responsable previamente lo recabe, los cuales son los siguientes:

a) Cuando sea necesario porque así lo ordena una ley;
b) Los datos personales se obtengan de una fuente de acceso público;
c) Cuando se realice un procedimiento previo de disociación de forma que no se pueda identificar su titular;
d) El tratamiento tenga el propósito de cumplir obligaciones de una relación jurídica entre el titular y el responsable;
e) Exista una situación de emergencia al individuo en su persona o en sus bienes;
f) Los datos personales sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria.
g) Se dicte resolución de autoridad competente.

Si nos encontramos en alguno de estos supuestos no será necesario la obtención del consentimiento, el tratamiento que se realiza en una relación jurídica entre el responsable y el titular, no se requerirá el consentimiento. El hecho de que no se requiera el consentimiento para el tratamiento, no implica que no se deberán cumplir los otros principios, lo que incluye la obligación de poner a disposición del titular el aviso de privacidad.

En el caso de tratar los datos personales para finalidades distintas, en ese supuesto se deberá solicitar el consentimiento de los titulares para las nuevas finalidades, además tener en cuenta los supuestos de excepción de que señala del artículo 10 de la LFPDPPP, antes citados.

---

su negativa para el tratamiento de sus datos de conformidad con lo anterior, se entenderá que ha otorgado su consentimiento para el tratamiento de los mismos, salvo prueba en contrario.
[…]

Si las nuevas finalidades requieren el consentimiento del titular, será necesario poner a su disposición un nuevo aviso de privacidad con la información relativa a las nuevas finalidades.[76]

Cuando no es necesario la obtención del consentimiento bastara con la actualización del aviso de privacidad e informar de los cambios al titular.

Los concesionarios de telecomunicaciones incumplen la normativa de protección de datos al no hacernos del conocimiento el cambio de las finalidades en el aviso de privacidad.

- **Principio de información**

Los responsables deben informar a los titulares de los datos personales, las características principales del tratamiento al que será sometida su información personal, ello se materializa a través de la puesta a disposición del aviso de privacidad, lo anterior de conformidad con el artículo 15 de la LFPDPPP. Todo responsable que trate datos personales, sin importar la actividad que realice o si se trata de una persona física o moral, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo.

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad.

La puesta a disposición del aviso de privacidad implica hacer del conocimiento del titular dicho documento, el responsable no está obligado a entregar una copia del aviso de privacidad al titular, al menos que éste lo solicite en ejercicio de su derecho de acceso.

[76] INAI. *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, disponible en http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf, p. 22

Es importante señalar que los responsables están obligados a comprobar o demostrar que han puesto a disposición del titular el aviso de privacidad, lo cual puede ser a través de los medios que estime pertinentes, como, por ejemplo, fotografías, grabaciones telefónicas, fe de hechos o firmas de los titulares, entre otros.

El responsable tiene la obligación de poner a disposición el aviso de privacidad cuando obtenga los datos personales de forma indirecta y sea con fines históricos, estadísticos o científicos[77]. En México el derecho a la protección de datos personales sólo aplica a personas físicas, de acuerdo con el artículo 3 fracción XVII de la LFPDPP solo son titulares las personas físicas. De conformidad con el artículo 2 de la LFPDPP, cuando se obtengan datos personales de personas para uso estrictamente personal y sin fines de divulgación comercial, tampoco será necesario poner a disposición el aviso de privacidad. Asimismo, de acuerdo a lo dispuesto en el artículo 5 del Reglamento de la LFPDPPP, no es aplicable a personas morales, personas físicas en su calidad de comerciantes y profesionistas y cuando se obtengan con fines de representación de personas físicas que prestan sus servicios a otras personas físicas o morales, relativos al nombre completo, puesto desempeñado, domicilio físico, correo electrónico, teléfono y número de fax.[78]

[77] LFPDPP. Artículo 18.- Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad.
No resulta aplicable lo establecido en el párrafo anterior, cuando el tratamiento sea con fines históricos, estadísticos o científicos.

[78] RLFPDPP.
Artículo 5. Las disposiciones del presente Reglamento no serán aplicables a la información siguiente:
I. La relativa a personas morales;
II. Aquélla que refiera a personas físicas en su calidad de comerciantes y profesionistas, y
III. La de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, consistente únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como algunos de los siguientes datos laborales: domicilio físico, dirección electrónica, teléfono y número de fax; siempre que esta información sea tratada para fines de representación del empleador o contratista.

- **Principio de calidad**

El principio de calidad se refiere a que los datos personales deben ser tratados exclusivamente conforme a la finalidad o finalidades para el cual fueron obtenidos.

Se refiere a una idea de racionalidad y proporcionalidad para que no hagan mal uso o manejo excesivo de nuestros datos, es una medida pertinente sobre el uso de los datos conforme a las finalidades que motivaron el tratamiento, por ello es necesaria una compatibilidad entre los datos solicitados y la finalidad de la recolección[79].

El Reglamento de la LFPDPPP en su artículo 36, señala las siguientes características a tomar en cuenta para el cumplimiento del principio de calidad.

a) Los datos personales son exactos cuando reflejan la situación de su titular, es decir su veracidad.
b) Son completos cuando los datos que se obtuvieron son los necesarios y falta ningún dato para las finalidades.
c) Son pertinentes cuando corresponden efectivamente al titular.
d) Los datos están actualizados cuando corresponden a una situación real y la información efectivamente corresponde al titular con el que está vinculado.
e) Por último, son correctos cuando tienen todas las características de ser exactos, completos, pertinentes y actualizados[80].

[79] Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (Infodf), op. cit, *p*p. 201 y 202

[80] Reglamento LFPDPP. Principio de calidad
Artículo 36. Se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.
Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga.
Cuando los datos personales no fueron obtenidos directamente del titular, el responsable deberá adoptar medidas razonables para que éstos respondan al principio de calidad, de acuerdo con el tipo de datos personales y las condiciones del tratamiento.
El responsable deberá adoptar los mecanismos que considere necesarios para procurar que los datos personales que trate sean exactos, completos, pertinentes, correctos y actualizados, a fin de

- **Principio de finalidad**

Los datos solo deben utilizarse para las finalidades que se informen en el aviso de privacidad y que fueron consentida por el titular. La finalidad del tratamiento es el motivo por el cual serán tratados los datos personales.

Las finalidades deben ser determinadas y especificar el motivo o el objeto para el tratamiento de forma clara.

De acuerdo con el artículo 41 Reglamento de la LFPDPPP, tenemos las finalidades que se pueden diferenciar entre las que son necesarias para la relación jurídica entre el titular y el responsable y las que no son necesarias por lo tanto la existencia no determina la relación jurídica.

- **Principio de lealtad**

De acuerdo con el artículo 7 de la LFPDPPP, en el tratamiento de los datos personales existe la expectativa razonable de privacidad, la cual debe ser entendida como la confianza que deposita una persona en otra y en donde se espera que los datos personales sean tratados conforme a lo convenido por las partes.

- El responsable debe utilizar los datos de manera lícita y leal, por lo que debe ser conforme a las leyes en general y en forma particular la normatividad sobre protección de datos personales. El responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido.
- De acuerdo con el principio de lealtad, la obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:

---

que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

- Está prohibida la obtención de los datos personales mediante el dolo, mala o negligencia; y
- El responsable deberá tratar los datos conforme a lo acordado, para no vulnerar la confianza del titular.

- **Principio de proporcionalidad**

El principio de proporcionalidad dispone la obligación del responsable de utilizar únicamente los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades.

Por ello será cuando se adquieren y se solicitan los datos personales requeridos para la prestación de un servicio, por lo tanto, no será correcto si se condiciona la la prestación del servicio con una finalidad diferente, sin que esto tenga nada que ver con la prestación inicial.

El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron.

De conformidad con el artículo 9 de la LFPDPPP, el responsable en el tratamiento de datos sensibles debe realizar esfuerzos razonables para limitar el periodo al mínimo indispensable, en este caso la Ley da una mayor protección y dispone en el caso de las bases de datos personales sensibles, se deben justificar la creación y las finalidades concretas y acordes con las actividades del responsable.

En ese sentido, sólo podrán crearse bases de datos personales sensibles cuando:
1. Obedezca a un mandato legal;
2. Se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o

3. El responsable lo requiere para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

De acuerdo al principio de proporcionalidad solo se deben usar los datos que son necesarios adecuados con relación a las finalidades, utilizar la menor cantidad de datos posible y limitar el periodo del tratamiento de datos personales. Si tomamos en cuenta este principio, nos damos cuenta que los concesionarios de telecomunicaciones violan este principio por que la relación jurídica es la prestación de un servicio de telecomunicaciones y sin embargo realizan la geolocalización, conservación, rastreo y almacenamiento de datos personales y dispositivos entre otras actividades.

- **Principio de responsabilidad**

El artículo 14 de la LFPDPPP, establece que los responsables del tratamiento están obligados a la protección de los datos personales de los titulares, sin importar que sean tratados por encargados (el encargado actúa a nombre y cuenta del responsable). Este principio supone que el responsable actué en los términos establecidos en el aviso de privacidad y sean respetados por aquéllos con los que mantenga una relación jurídica.[81]

Es la obligación de los responsables de verificar el cumplimiento del resto de los principios y adoptar las medidas necesarias para su aplicación, y en su caso demostrar ante los titulares y la autoridad, el cumplimiento de sus obligaciones.

[81] LFPDPPP. Artículo 14.- El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.

De acuerdo con el artículo 48 del Reglamento de la LFPDPPP, el responsable debe crear las acciones necesarias para garantizar el debido tratamiento entre ellas las siguientes:

a) Elaborar políticas y programas de privacidad obligatorios dentro de la organización del responsable.
b) Implementar programas de capacitación, actualización y concientización al personal sobre las obligaciones en materia de protección de datos personales.
c) Establecer mecanismos de supervisión y vigilancia interna para comprobar el cumplimiento de las políticas de privacidad;
d) Instrumentar un procedimiento que atienda el riesgo para la protección de datos personales.
e) Revisar periódicamente las políticas y programas de seguridad.
f) Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;
g) Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.
h) El responsable puede optar por medidas adicionales o distintas que contribuyan a elevar los estándares de protección de datos personales y cumplir con la normativa que regula este derecho.

- **Deber de confidencialidad y seguridad**

Además de la obligación de cumplir los principios la LFPDPPP señala el deber de confidencialidad y de seguridad. La confidencialidad se trata de una obligación de guardar secreto de los datos personales que son o fueron utilizados con el objetivo de evitar un daño a su titular[82]. También, sirve para evitar que un tercero no autorizado tenga acceso a cualquier información.

[82] Sánchez Hernández, Néstor Mauricio, *El derecho al acceso a la información y la protección de datos personales*, México, INAI, 2016, p. 42

El responsable tiene la obligación de adoptar las medidas para evitar que se divulgue la información, incluso persiste la obligación de guardar confidencialidad una que se termine la relación jurídica entre el responsable y sobre quien tenga acceso a los datos personales en respecto a las funciones encomendadas. Asimismo, esa confidencialidad debe existir una vez concluida la relación jurídica entre el titular y el responsable.

Este deber debe contener las medidas de seguridad tanto técnicas, físicas y administrativas, para la protección de los datos personales contra cualquier daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

El otro deber se refiere a la obligación de establecer medidas de seguridad para proteger los datos con cualquier daño, perdida, alteración, destrucción o el uso, acceso o tratamiento indebido o no autorizada. Las medidas de seguridad pueden ser técnicas, físicas y administrativas.

- **Derechos ARCO**

El artículo 16 de la CPEUM, reconoce que toda persona tiene derecho a la protección de sus datos personales, acceso, rectificación, cancelación, así como a manifestar su oposición[83] y la LFPDPPP reconocen los siguientes derechos a los titulares de los datos personales:

Acceso: Consiste en el derecho del titular de conocer que datos utiliza o almacena el responsable, en sus bases de datos, registros, expedientes o sistemas, así como de conocer que uso le da a su información personal.

[83] CPEUM. Artículo 16, segundo párrafo:
[…]
Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
[…]

> *Rectificación:* Es el derecho del titular de *solicitar la rectificación o corrección* de sus datos personales, cuando éstos resulten inexactos o incompletos o no se encuentren actualizados. En otras palabras, el titular puede solicitar a quien posea o utilice sus datos personales que los corrija cuando los mismos resulten ser incorrectos, desactualizados o inexactos[84].

Cancelación: Cuando el titular solicita que sus datos personales sean eliminados de las bases de datos, sistemas, expedientes, no es todos los casos es procedente la eliminan debido a que son necesarios conservar por disposiciones legales o porque son necesarios para la relación jurídica.

> *Oposición: Es el derecho del titular de solicitar que sus datos personales no se utilicen para ciertos fines, o de requerir que se termine el uso de los mismos. También en este caso, no siempre se podrá impedir el uso de los datos personales, principalmente cuando sean necesarios por alguna cuestión legal o de cumplimiento de obligaciones*[85]*.*

El derecho a la protección de datos personales solo es procedente a solicitud del titular de los datos personales o, en su caso, su representante, podrán solicitar el ejercicio de los derechos ARCO.

Al respecto, los responsables del tratamiento están obligados a:

- Designar a una persona o departamento de datos personales, para dar trámite a las solicitudes de ejercicio de derechos ARCO de los titulares, así como para fomentar la protección de los datos personales al interior de la organización;

[84] INAI. Guía para titulares de los datos personales. Volumen 3. Disponible en http://inicio.inai.org.mx/GuiasTitulares/Guia%20Titulares-03_PDF.pdf p. 6
[85] Ibidem, p. 7

- Implementar medios y mecanismos para que los titulares ejerzan sus derechos ARCO;
- Conservar los datos personales de forma tal que permitan el ejercicio de los derechos ARCO por parte de los titulares, y
- Atender las solicitudes de derechos ARCO en los plazos y bajo las reglas que establezca la normatividad aplicable a la materia.

Ahora bien, como todo derecho, el de protección de datos personales tiene límites, el mismo artículo 16 de la CPEUM, la ley podrá establecer supuestos de excepción por razones de *seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.* También, el artículo 4 de la LFPDPPP señala como límites la protección a la seguridad nacional, seguridad y salud públicos, así como los derechos de terceros.

5. Convención Interamericana de Derechos Humanos

El Sistema Interamericano de Derechos Humanos es un sistema regional que promueve la protección de derechos humanos el cual está compuesto por dos órganos: la Comisión Interamericana de Derechos Humanos (en lo sucesivo la Comisión Interamericana) y la Corte Interamericana de Derechos Humanos (en lo sucesivo la Corte Interamericana).

La Comisión Interamericana se encarga de la defensa de los derechos humanos, por ello realiza visitas a los países, actividades e informes de la situación de los derechos humanos sobre temas en general o particular y realiza medidas cautelares o provisionales. Por su parte la Corte Interamericana realiza el análisis de peticiones con la finalidad de determinar la responsabilidad internacional por violaciones a los derechos humanos, se deben agotar los recursos judiciales del Estado de que se trate.

En términos generales, la Comisión Interamericana tiene como atribuciones relevantes dar seguimiento a los programas que realizan los Estados para cumplimiento de la Convención, por lo cual recibe informes, realiza estudios y hace recomendaciones; la segunda será recibir de cualquier persona o entidades no gubernamentales peticiones sobre la presunta violación de los derechos contenidos en la Convención cometidos por un Estado parte[86].

Con la implementación del sistema interamericano nuestro país le ha dado la importancia a las normas internacionales de derechos humanos, muchos cambios normativos e institucionales se deben a las recomendaciones de la Comisión Interamericana, con la reforma Constitucional el artículo primero incorpora los derechos humanos y cambia el concepto tradicional de garantías individuales[87].

La incompatibilidad del derecho interno (Constitución, ley, actos administrativos, jurisprudencia, prácticas administrativas y judiciales, etc.), sucede cuando el Estado promulgué normas que violen los derechos humanos, no realicé las medidas para garantizar tales derechos o no se deroguen las normas contrarias.[88]

Con el sistema interamericano en el momento que Estado reconoce derechos humanos adquiere obligaciones internacionales *erga omnes,* por lo que debe respetar y garantizar su libre y pleno ejercicio.

Los derechos humanos se presentan en toda la administración pública, en todos sus niveles, y obliga a todas las autoridades no solo de respetarlos también de interpretar para maximizar el goce de los derechos[89]. La SCJN ha reiterado que los

[86] Soberanes, José Luis, *Derechos humanos y su protección constitucional*, México, Porrúa, 2012, p. 38
[87] Jardón Piña, Luis Manuel, *Criterios y jurisprudencia interamericana de derecho humanos: Influencia y repercusión en la justicia penal*, México, Instituto de Formación Profesional de la Procuraduría General de Justicia del Distrito Federal, 2014, p. 338
[88] Ferrer Mac-Gregor, Eduardo y Zaldívar Lelo de Larrea, Arturo (Coord), *La Ciencia del Derecho Procesal Constitucional,* Tomo IX, Derechos Humanos y Tribunales Internacionales*,* México, Instituto de Investigaciones Jurídicas, UNAM, 2008, p. 226 y 227
[89] Jardón Piña, Luis Manuel, op. Cit., p. 339

derechos humanos se interpretarán de conformidad con la propia Constitución y con los tratados internacionales de la materia, favoreciendo en todo tiempo a las personas la protección más amplia[90].

A través del artículo 1º Constitucional, tenemos que las normas relativas a los derechos humanos se interpretarán de conformidad con ésta y con los tratados internacionales suscritos y ratificados por el estado mexicano, favoreciendo en todo tiempo la protección más amplia a las personas, en la protección y defensa de los derechos humanos reconocidos en la Constitución General.

Lo anterior tiene sustento en los atributos de la persona humana, en donde el ser humano tiene una protección internacional de naturaleza convencional o complementaria al derecho interno. La SCJN ha determinado que la aplicación del control difuso de convencionalidad se realiza en suplencia de la normativa interna, esto es, el juzgador previo a realizar un control de convencionalidad, en el ámbito de sus competencias, primero debe analizar las reglas y principios del derecho interno, y acudir directamente a la normativa internacional. En ese contexto, si se determina que el derecho interno no otorga las garantías suficientes para velar por

[90] CONTROL DE CONSTITUCIONALIDAD Y CONVENCIONALIDAD. CONDICIONES PARA SU EJERCICIO OFICIOSO POR LOS ÓRGANOS JURISDICCIONALES FEDERALES.
El párrafo segundo del artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos dispone que las normas relativas a los derechos humanos se interpretarán de conformidad con la propia Constitución y con los tratados internacionales de la materia, favoreciendo en todo tiempo a las personas la protección más amplia, de donde deriva que los tribunales federales, en los asuntos de su competencia, deben realizar el estudio y análisis ex officio sobre la constitucionalidad y convencionalidad de las normas aplicadas en el procedimiento, o en la sentencia o laudo que ponga fin al juicio. Ahora, esta obligación se actualiza únicamente cuando el órgano jurisdiccional advierta que una norma contraviene derechos humanos contenidos en la Constitución Federal o en los tratados internacionales de los que el Estado Mexicano sea parte, aun cuando no haya sido impugnada, porque con su ejercicio oficioso se garantiza la prevalencia de los derechos humanos frente a las normas ordinarias que los contravengan. De otra manera, el ejercicio de constitucionalidad y convencionalidad de normas generales no tendría sentido ni beneficio para el quejoso, y sólo propiciaría una carga, en algunas ocasiones desmedida, en la labor jurisdiccional de los Jueces de Distrito y Magistrados de Circuito. Tesis 2a./J. 69/2014 (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. I, junio de 2014, p. 555.

la protección de los derechos humanos, se justificara el control difuso de convencionalidad.[91]

Tomando en consideración el sistema interamericano los Estados deben proteger y establecer un régimen en la vida privada de las personas, para regular el almacenamiento, procesamiento, uso y transferencia de los datos personales.

---

[91] CONTROL DIFUSO DE CONVENCIONALIDAD EX OFFICIO. SU APLICACIÓN ES DE NATURALEZA SUBSIDIARIA O COMPLEMENTARIA DEL SISTEMA JURÍDICO MEXICANO.
De la interpretación sistemática y teleológica de los principios pro persona establecido en el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, que dispone que las normas relativas a los derechos humanos se interpretarán de conformidad con ésta y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia, hermenéutico en materia convencional, previsto en el preámbulo de la Convención Americana sobre Derechos Humanos, que reconoce que los derechos esenciales del hombre no nacen del hecho de ser nacional de determinado Estado, sino que tienen como sustento los atributos de la persona humana, razón por la cual justifican una protección internacional, de naturaleza convencional coadyuvante o complementaria de la que ofrece el derecho interno de los Estados Americanos, se advierte que la aplicación del control difuso ex officio en materia de derechos humanos es una herramienta de interpretación subsidiaria o complementaria del sistema jurídico mexicano, cuyo uso está condicionado a la optimización de la norma que la integra para maximizar la defensa de los ciudadanos cuando el derecho interno no alcanza para ese fin. Esto significa que la aplicación del mencionado control se realiza en suplencia de la deficiencia de la normativa interna; es decir, el juzgador no debe acudir directamente a la normativa internacional para buscar respuesta al asunto, en virtud de que, antes, por lógica y preferencia del derecho interno, deberá analizar cómo está establecido el derecho humano en controversia en los contenidos que existen en las reglas y los principios constitucionales, así como en la legislación ordinaria, para que, una vez que se determine mediante los razonamientos respectivos que el derecho fundamental no está protegido o, si lo está, no suficientemente en favor de la persona, se justifica que se realice el control difuso de convencionalidad ex officio. De no hacerse así, éste pudiera aplicarse sin restricción alguna, acudiendo de manera directa a la normativa internacional para resolver el caso, sin antes ponderar y justificar la insuficiencia o imperfección del derecho interno, pues no debe soslayarse que el sistema jurídico de cada Estado presenta características especiales que lo distinguen, por lo que de acuerdo a su situación, cada Nación deberá establecer cómo aplicar el control difuso de convencionalidad que lo haga coherente con su derecho interno y, como consecuencia, que se logre la optimización de los derechos humanos. Además, es importante establecer que el sistema nacional prevé una serie de formalidades e instancias para que el gobernado haga valer sus derechos y se reparen sus posibles violaciones; por lo que si se acudiera directamente al control difuso de convencionalidad, se provocaría desorden e incertidumbre en la aplicación del derecho para la solución de los casos, pues podría pasar que existiendo solución en la normativa interna y sin agotarse sus recursos o instancias, se aplicara la normativa internacional, dispensando a la persona del cumplimiento de las cargas que le correspondían de acuerdo con el orden jurídico nacional, lo que es irrealizable y agrede la coherencia y la funcionalidad del sistema interno; máxime que la Constitución Federal, en su artículo 1o., condiciona que dicho control sea útil para optimizar el derecho humano, lo que constituye un presupuesto constitucional previo que el aplicador deberá ponderar para estar en condiciones de realizar o no el control citado. Tesis: Jurisprudencia (III Región) 5o. J/8 (10a.), *Gaceta del Semanario Judicial de la Federación,* Décima Época, t. II, 4 marzo de 2014, p. 1360

6. Directiva 2006/24/CE Del Parlamento Europeo

Para la implementación de un sistema de protección de datos personales, consideramos que debió tomarse en consideración la *Directiva 2006/24/CE Del Parlamento Europeo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.*

Al igual que nuestro Sistema Interamericano, los Estados deben proteger los derecho y libertades de lo relativo al tratamiento de los datos personales y el derecho a la intimidad[92].

En la Directiva *2006/24/CE* se señala el objetivo de dar cumplimiento al artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, donde se señala que toda persona tiene derecho al respeto a su vida privada, cualquier injerencia o intervención deberá estar prevista por la ley, que justifique su implementación en una sociedad democrática, entre otras la seguridad nacional, la seguridad pública, la prevención de delitos, la protección de los derechos y las libertades de terceros.

Vemos que la conservación de datos se creó como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, sin embargo, para garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo, se estableció la Directiva *2006/24/CE* para establecer condiciones para

[92] Directiva 2006/24/CE del Parlamento Europeo y del Consejo del 15 de marzo de2006, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*, disponible en: https://www.boe.es/doue/2006/105/L00054-00063.pdf

no vulnerar el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales .[93]

De acuerdo al Considerando 13 de la Directiva 2006/24/CE, se trata solo de datos generados a través de una comunicación, se debe prever que no sean conservados más de una vez y la información que deriva de la prestación de servicios de comunicaciones electrónicas. En cuanto a correos electrónicos y telefonía, la obligación de conservar datos sólo puede aplicarse con respecto a los datos de los servicios propios de los proveedores[94].

La información debe conservar exclusivamente los datos generados como parte del suministro del servicio de comunicación, si no fueron generados por el proveedor no es obligatorio conservarlos.

En su artículo primero la Directiva, pretende la armonización de los Estados miembros sobre las obligaciones a los proveedores de servicios de comunicaciones electrónicas, para que solo se utilicen con fines de investigación y detención de delitos graves.

De acuerdo al artículo 6, los Estados tomaran medidas como establecer un periodo de conservación de seis meses como mínimo y máximo de dos años a partir del día de la comunicación.

En su artículo 7, se prevé la protección de los datos personales en cuestiones de seguridad de los datos como son:

---

[93] Directiva 2006/24/CE del Parlamento Europeo y del Consejo del 15 de marzo de2006, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*, disponible en: https://www.boe.es/doue/2006/105/L00054-00063.pdf

[94] Directiva 2006/24/CE del Parlamento Europeo y del Consejo del 15 de marzo de2006, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*, disponible en: https://www.boe.es/doue/2006/105/L00054-00063.pdf

a) Que los datos conservados tendrán la misma calidad y gozarán de la mismas normas y protección de seguridad;
b) Los datos contaran con las medidas técnicas para su protección en caso de destrucción accidental o ilícita, perdida, alteración, almacenamiento, tratamiento, acceso o divulgación no autorizados.
c) Los datos estarán sujetos a medidas técnicas en donde solo pueden acceder a ello las personas autorizadas, y
d) Los datos se destruirán al periodo de conservación con la excepción que aquellos que fueron objeto de acceso.

7. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo del 27 de abril de 2016.

Esta directiva fue creada con la finalidad de garantizar la cooperación penal y judicial entre Estados, crear un nivel adecuado sobre la protección de datos personales y facilitar el intercambio de datos personales, otro objetivo es garantizar la protección eficaz de los datos personales en toda la Unión Europea requiere tanto el fortalecimiento de los derechos de los interesados y de las obligaciones de quienes tratan dichos datos personales. Mediante una armonización en las normas para la protección y la circulación de los datos personales con fines de prevención, investigación, detección de cuestiones penales y seguridad pública.

La protección de las personas físicas en relación con el tratamiento de los datos de carácter personal es un derecho fundamental, lo cual se encuentra en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europeo. Los

principios y normas de protección deben respetar las libertades y derechos fundamentales.

Para las cuestiones de cooperación judicial en materia penal y policial, se necesita un nivel elevado de protección. En materia de prevención, investigación, detección o enjuiciamiento de infracciones penales, también deben aplicarse los principios de la protección de datos deben a toda la información relativa a una persona física identificada o identificable.

Las autoridades competentes para la seguridad del tratamiento de los datos personales deben garantizar un nivel adecuado de seguridad y confidencialidad, entre ellas deben impedir el acceso particular impidiendo el acceso sin autorización o cuidad el uso no autorizado, así como las medidas físicas del equipo utilizado en el tratamiento y tomando en consideración la naturaleza de los datos personales que tienen que protegerse.

Los datos personales deben obtenerse para fines determinados, explícitos y legítimos, exclusivamente para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública.

El responsable debe hacer una evaluación sobre los riegos y tomar acciones para mitigarlos, el nivel de seguridad y confidencialidad debe ser adecuado respecto al riesgo y naturaleza de los datos personales que deben protegerse. En la evaluación de impacto debe tomarse en cuenta la posibilidad de la destrucción, la pérdida, la alteración o comunicación no consentida. Así como cerciorarse que el tratamiento no debe llevarse a cabo por personas no autorizadas[95].

[95] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES

La seguridad del tratamiento de los datos personales de acuerdo al artículo 29, exige que los responsables y encargados deben tomar en consideración la técnica, los costos, la naturaleza, el alcance, el contexto y los fines del tratamiento. Para garantizar la protección de los datos personales, en cuanto al tratamiento automatizado, se poner en práctica medidas destinadas a las siguientes acciones:

a) No permitir el acceso a personas no autorizadas, incluyendo el acceso a los equipos.
b) Que lo datos no puedan ser leerse, copiarse o modificarse por personas no autorizadas.
c) No permitir sin la debida autorización la introducción de datos personales conservados.
d) Que se cuente con las medidas para evitar uso no autorizado por medo de trasmisión de datos, esto se refiere a un control de los usuarios.
e) Las personas autorizadas solo tengas acceso a los datos para los cuales tienen autorización.
f) La posibilidad de verificar a que instituciones u organismos se han trasmitidos los datos.
g) Que se posible verificar quienes se introducen en los sistemas.
h) Evitar que los datos puedan ser leídos, copiados o modificados durante las trasferencias.
i) Garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.
j) Garantizar el correcto funcionamiento del sistema.

8. Sentencia del Tribunal de Justicia Europeo

Con fecha 8 de abril de 2014 el Tribunal de Justicia Europeo, se pronunció respecto a la validez de Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación

con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

La Litis se inició por parte de la empresa Digital Rights Ireland Ltd. (en lo sucesivo, Digital Rights) y las diversas instituciones del gobierno irlandés entre otras, el Minister for Communications y Marine and Natural Resources, en relación con la legalidad de medidas legislativas y administrativas nacionales sobre la conservación de datos relativos a comunicaciones electrónicas.

Otra petición fue la planteada por Verfassungsgerichtshof, concierne a recursos de inconstitucionalidad interpuestos, respectivamente, ante ese órgano jurisdiccional por el Kärntner Landesregierung (Gobierno del Land de Carintia) y por los Sres. Seitlinger, Tschohl y otros 11128 demandantes sobre la compatibilidad de la Ley por la que se transpone la Directiva 2006/24 en el ordenamiento jurídico austriaco con la Ley constitucional federal (Bundes-Verfassungsgesetz)[96].

En el caso de Verfassungsgerichtshof se pide a la Directiva 2006/24 un análisis de compatibilidad, en la medida que permite el almacenamiento en masa de datos con respecto a un número ilimitado de personas durante un período extenso (dos años). La conservación de datos afecta a personas cuyo comportamiento no justifica en modo alguno la conservación de datos referentes a ellas. Asimismo, las personas están expuestas al riesgo de que las autoridades investiguen nuestros datos, conozcan sobre nuestra vida privada y utilicen esos datos para múltiples fines, además de un número incontable de personas que tienen acceso a los datos durante un período mínimo de seis meses. La duda se refiere a si esta Directiva

[96] Sentencia del Tribunal de Justicia de fecha 8 de abril de 2014. Directiva 2006/24/CE — Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones — Conservación de datos generados o tratados en relación con la prestación de tales servicios — Validez — Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea. Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&qid=1487100101393&from=ES

logra los objetivos que persigue y si se justifica la injerencia en los derechos fundamentales afectados[97].

Los datos que deben conservar los proveedores de servicios de comunicaciones, son datos necesarios para rastrear e identificar el origen de una comunicación y el destino final, identifican la fecha, hora y duración, datos de edificación y localización del equipo móvil, nombre y dirección de usuario. Todos estos datos permiten saber con qué personas nos comunicamos, pueden determinar el momento y lugar en el que se realizó la comunicación, además la frecuencia de comunicaciones con determinadas personas en un periodo concreto.

Es preocupante como el uso de estos datos en su conjunto permite conclusiones sobre la vida privada de las personas, como nuestros hábitos personales, lugares de residencia, desplazamientos diarios, actividades realizadas, relaciones sociales y lugares sociales a los que acudimos.

Este tratamiento de datos permite el acceso a las autoridades, esto afecta de forma directa a la vida privada, por lo tanto, debe cumplir con los requisitos en materia de protección datos personales. La obligación impuesta a los proveedores de telecomunicaciones de conservados datos referentes a la vida privada y sus comunicaciones, constituye una injerencia a sus derechos[98].

De acuerdo al principio de proporcionalidad se establece que los actos del Estado deben ser adecuados conforme a los objetivos legítimos y no excedan los límites de lo que se considera apropiado o para el logro de dichos objetivos.

Respecto a si la conservación de datos es adecuada, es importante señalar que de acuerdo al creciente uso de la tecnología de la información permiten a las

[97] Idem
[98] Idem

autoridades la persecución de los delitos graves y constituye una herramienta útil para las investigaciones penales.

En cuanto a si es necesaria la conservación de datos, es importante para garantizar la seguridad pública y su eficacia depende de la técnica moderna de investigación. Sin embargo, este objetivo de interés general, no puede por sí solo justificar que una medida de conservación y sea considere necesaria para lucha de delitos graves. Se deben establecer reglas específicas sobre el alcance y establecer exigencias mínimas para proteger los datos de forma eficaz contra el abuso y utilización ilícita.

La Directiva 2006/24 *abarca de manera generalizada a todas las personas*, y cualquier medio de comunicación sin diferenciación, limitación o excepción de acuerdo al objetivo de delitos graves. Afecta todas las personas que utilizan servicios de comunicaciones, sin que se encuentren relacionadas con una situación de acciones penales, sin que existan indicios de un comportamiento relacionado con delitos graves. Al no establecer excepciones se aplica a personas que están sujetas al secreto profesional.

No se confirma la existencia de una relación entre la conservación de datos y una amenaza a la seguridad pública, porque no se refiere a un periodo o zona geográfica determinada o un circulo de personas implicadas en delitos graves.

No se menciona un criterio que permita delimitar el acceso a las autoridades y evitar su posterior utilización con fines prevención o enjuiciamiento.

No hay un número específico de *personas que disponen de la autorización de acceso* a los datos conservados conforme a lo estrictamente necesario, no se realiza un control previo de un órgano jurisdiccional o un organismo administrativo autónomo, con el objeto limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo perseguido.

Por lo que refiere al período de conservación de los datos, la Directiva 2006/24 establece un período mínimo de seis meses sin que se establezca ninguna distinción entre las categorías como son datos necesarios para rastrear e identificar el origen de una comunicación, datos para identificar el destino, datos para identificar la fecha y hora de la llamada entre otras.

Respecto a las reglas de *seguridad y a la protección de los datos conservados* por parte de los proveedores, no se garantiza una protección de los datos conservados contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos respecto de tales datos. No se da especial protección a los datos personales de carácter sensible y al riesgo en caso de acceso ilícito.

Debido a que no se garantiza un nivel elevado de protección y seguridad, sino que autoriza a dichos proveedores al establecimiento conforme a sus capacidades económicas, *no garantiza la destrucción definitiva de los datos al término de su período de conservación*.

CAPÍTULO TERCERO. LA CONSERVACIÓN DE DATOS PERSONALES EN MÉXICO

1. Conservación de los Datos Personales de acuerdo a la Ley Federal de Telecomunicaciones y Radiodifusión.

De acuerdo a la exposición de motivos de la Ley Federal de Telecomunicaciones y Radiodifusión, se proponía modificar el marco normativo vigente que permita interferencias con el derecho a la privacidad de las comunicaciones, el marco normativo vigente obliga a los concesionarios a llevar un registro hasta por 2 años, sin establecer ningún tipo de restricciones, como son un control judicial.

Se menciona que la obligación de conservación de datos o “retención de datos” contraviene el derecho a la inviolabilidad de las comunicaciones reconocido en el artículo 16 constitucional, así como en los tratados internacionales en materia de derechos humanos.

La protección a las comunicaciones se extiende a los “datos de tráfico de comunicaciones”, y la intervención se debe someter a los requisitos de la Constitución y los tratados internacionales, como son la autorización por parte de la autoridad judicial federal, requisitos de legalidad, fin legítimo y necesidad, lo cual implica el uso de medidas como la transparencia y la supervisión independiente por parte de un ente externo. La “retención de datos” es considerada contraria al derecho a la privacidad por organismos internacionales en materia de derechos humanos.

La idea era la creación de un marco que respetara los derechos humanos, señalan un marco conceptual sobre la aplicación de derechos humanos sobre la vigilancia de las comunicaciones. Entre los requisitos que debían integrarse de acuerdo a la exposición de motivos encontramos *legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, control judicial, debido proceso, notificación al usuario,*

transparencia, supervisión pública independiente, integridad de las comunicaciones y sistemas, entre otros. Por ello no creemos que se regula de manera adecuada el derecho a la privacidad de los usuarios y sus comunicaciones[99].

Como señalamos 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) obliga a los concesionarios a conservar por 24 meses una serie de datos de comunicaciones comúnmente conocidos como "metadatos de comunicaciones" o "datos de tráfico de comunicaciones" dentro de lo que la ley llama "Registro de Comunicaciones". Los datos conservarse son los siguientes:

- Nombre, denominación o razón social y domicilio del suscriptor;
- Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);
- Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;
- Datos necesarios para determinar la fecha, hora y duración de la comunicación,
- así como el servicio de mensajería o multimedia;
- Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;
- En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

[99] Gaceta Parlamentaria, año XVII, número 3916-V, jueves 28 de noviembre de 2013, *Proyecto de Decreto por el que se expide la Ley Federal de Telecomunicaciones y Radiodifusión, (Exposición de Motivos)*, disponible en http://gaceta.diputados.gob.mx/Gaceta/62/2013/nov/20131128-V.html#Iniciativa3

- La ubicación digital del posicionamiento geográfico de las líneas telefónicas.

Este tipo de obligaciones de la *conservación de datos ha sido rechazada por organismos internacionales de protección de derechos humanos*, es evidente la interferencia en la privacidad de millones de personas, en contravención a los principios de necesidad y proporcionalidad.

El proyecto de ley represento amenazas a los derechos humanos, como señaló la Comisión de Derechos Humanos de la Ciudad de México, a pesar de los cambios realizados. Como ya lo señalamos en abril de 20014 el Tribunal de Justicia de las Comunidades Europeas señalo que la retención de datos por parte de concesionarios para la investigación de delitos es violatoria de los derechos humanos debido a que no cumple con el principio de proporcionalidad[100].

Para la protección de la privacidad de los usuarios debemos aplicar las siguientes recomendaciones:

a) Libre circulación de ideas y no injerencias

Si todas las personas tienen derechos a las telecomunicaciones, estas deben prestarse sin injerencias arbitrarias, por eso están prohibidas las restricciones a la libre expresión, transmisión y circulación de ideas y opiniones.[101] Se ha considerado que con la conservación de datos las personas se sienten vigiladas, ello provoca una restricción a la libertad de expresión.

b) No intervenciones de comunicaciones privadas

Todos los usuarios de telecomunicaciones en la República mexicana tienen el derecho a que sus comunicaciones privadas sean libres y se respete su privacidad.

[100] Álvarez, Clara Luz, *Mexican Telecom Reform: Private Interest First",* México, Instituto de Investigaciones Jurídicas UNAM, Volumen 8, Número 1, México jul./dic. 2015, p. 70
[101] Álvarez, Clara Luz, *Derechos de los usuarios de telecomunicaciones*, op. cit., p. 4

Las comunicaciones pueden ser telefónicas, por video, mensajes de texto y multimedia, mensajes de correo electrónico, mensajería instantánea (chats) entre otras. Solamente previa autorización de un juez federal se puede intervenir una comunicación privada.[102]

Cuando las autoridades requieran la información conservada deberán realizar una autorización judicial federal previa. Las solicitudes de autorización judicial deben señalar los fundamentos legales, el tipo de intervención, los sujetos y su duración. Se **prohíbe** la intervención de comunicaciones privadas en cuestiones de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, o el supuesto de las comunicaciones del detenido con su defensor[103].

c) Derechos de los usuarios de telecomunicaciones.

El usuario tiene las opciones limitadas para seleccionar al proveedor de servicios, y deben aceptar los contratos de adhesión por lo tanto el usuario no puede negociar, porque son contratos tipo[104].

Sobre la protección de datos y la privacidad, se cuenta con el derecho a recibir información sobre los riesgos y medidas. Y la obligación de los concesionarios de informar un incidente o una vulneración en la red a los usuarios[105].

2. Excepciones a la privacidad

La privacidad como derecho fundamental está consagrado en el Sistema Interamericano de Derechos Humanos, debido al desarrollo tecnológico se tiene un

[102] Ibidem, p. 9
[103] Red en Defensa de los Derechos Digitales, op. cit., p. 19
[104] Álvarez, Clara Luz, *Derechos de los usuarios de telecomunicaciones*, op. cit., p. 25
[105] Ibidem, p. 30

tratamiento intensivo sobre las personas, del cual surgió la autodeterminación como el poder de decir sobre quien, cuando, como y para que utiliza la información[106].

El tratamiento de datos personales se regula bajo estándares internacionales que permiten garantizar a las personas la confidencialidad y la seguridad de la información, pero al mismo tiempo se permite una correcta y adecuada trasmisión de la información[107].

El artículo 16 constitucional exige que toda intervención de comunicaciones privadas debe contar con una autorización judicial federal previa. La SCJN, al interpretar dicho artículo en el Amparo en Revisión 964/2015, concluyó que las autoridades que pretendan llevar a cabo medidas de vigilancia de comunicaciones, deben cumplir el requisito de autorización judicial federal previa tanto para la vigilancia del contenido de comunicaciones, como de los "metadatos de comunicaciones".

En la resolución de la acción de Inconstitucionalidad 32/2012, se establece que la finalidad de la geolocalización es la persecución de los delitos,[108] en consecuencia, la conservación de datos tiene la misma finalidad como una actividad y diligencia en la investigación de hechos probablemente constitutivos de delitos.

El pleno de la Suprema Corte de Justicia de la Nación al resolver la acción de inconstitucionalidad 32/2012 determinó que la geolocalización se refiere a los equipos de comunicación móvil y no a personas, y no constituye una restricción a la vida privada de las personas, ya que no se encuentra dirigida a buscar personas sino un instrumento del delito[109].

---

[106] Peschard Mariscal, Jacqueline, *Protección de Datos Personales. La voz de los actores,* México, Instituto Federal de Acceso a la Información Pública, 2010, p. 19
[107] Ibidem, p. 20
[108] Flores Pacheco, Moisés Israel, "La geolocalización y el derecho a la privacidad. Análisis de la Acción de Inconstitucionalidad 32/2012*"*, *Estudios en Derecho a la Información,* México, Instituto de Investigaciones Jurídicas UNAM, Número 1, ene/jun. 2016, p. 80
[109] Flores Pacheco, Moisés Israel, op. cit., p. 88

> La lectura de las disposiciones legales cuestionadas, permite establecer que la solicitud que dirige el Procurador General de la República, o las personas en quienes delegue esta facultad, a concesionarios o permisionarios del servicio de telecomunicaciones, se contrae a la ubicación del lugar en el momento preciso en que se procesa la búsqueda, de un equipo terminal móvil, asociado a una línea telefónica determinada. Esto es, tiene por objeto *conocer el lugar aproximado desde el cual se origina una llamada proveniente de un teléfono móvil*, asociado a una línea determinada o identificada.
>
> La medida, entonces, se constriñe a tal objeto y procede sólo en caso de que los equipos móviles, asociados a una línea, se encuentren relacionados en las investigaciones de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas.
>
> En consecuencia, se trata, en principio, de la localización de un equipo terminal móvil asociado a una línea telefónica determinada en el momento en que se procesa la búsqueda, y *no así de la intervención de las comunicaciones* que se realicen a través de tales equipos, ni siquiera del registro de las llamadas.
>
> Con independencia de que, con posterioridad, y como consecuencia lógica, una vez ubicado el lugar que se busca, se pueda identificar la persona que detenta o hace uso del equipo para realizar llamadas, y determinar las medidas que -en su caso- procedan en el curso de la investigación de que se trata y los elementos que aporte su localización[110].

No estamos de acuerdo con esta concepción de la corte al final se pueden obtener datos sobre las personas, con quienes se comunica, lugares que frecuenta, estos metadatos en su conjunto generan un perfil sobre la identidad de la persona.

Solo establecieron como limitantes a la atribución del Ministerio Público, la obligación de dejar constancia de la solicitud en el expediente de la investigación y

[110] CNDH. Acción de Inconstitucionalidad 32/2010, disponible en http://www.cndh.org.mx/sites/all/doc/Acciones/Acc_Inc_2012_32_Demanda.pdf p. 78 y 79

motivar el requerimiento de extrema urgencia[111], cuando acredite los siguientes supuestos:

- Se encuentre en riesgo la vida o la integridad física.
- Pueda ocultarse o desaparecer el objeto de la investigación.
- En delitos como secuestro, amenazas, crimen organizado, delitos contra la salud o extorsión.

3. Jurisprudencia SCJN

La jurisprudencia nos da un panorama sobre la aplicación de LFTR, por ello se ha considerado que los concesionarios de telecomunicaciones no son autoridad responsable para efecto del juicio de amparo, el registro y control de las comunicaciones de sus usuarios son obligaciones frente a las autoridades de seguridad, procuración y administración de justicia. Los concesionarios no actúan como autoridades responsables (ejecutoras), no tienen una atribución, sino una obligación, lo hacen en colaboración con la autoridad, tal y como lo señala la siguiente tesis:

> CONCESIONARIOS DE TELECOMUNICACIONES. NO SE CONSTITUYEN COMO AUTORIDAD RESPONSABLE PARA EFECTOS DEL JUICIO DE AMPARO CUANDO ACATAN LOS LINEAMIENTOS DE COLABORACIÓN EN MATERIA DE SEGURIDAD Y JUSTICIA (A TRAVÉS DE LOS CUALES SE REGULAN LOS ARTÍCULOS 189 Y 190 DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN), PORQUE ACTÚAN COMO AUXILIARES DEL ENTE ESTATAL. De los criterios jurisprudenciales emitidos por la Suprema Corte de Justicia de la Nación en relación con el artículo 5o., fracción II, párrafo segundo, de la Ley de Amparo, deriva que para que un particular tenga calidad de autoridad responsable es menester la satisfacción de las siguientes condiciones: a) Que dicte, ordene, ejecute o trate de ejecutar actos que creen, modifiquen o extingan situaciones jurídicas; b) Tal afectación sea unilateral y obligatoria, es decir, sin que al efecto se requiera acudir a los órganos judiciales ni se precise del consenso de la voluntad del afectado; c) El acto derive de funciones determinadas por una norma, por lo que resulte de ejercicio irrenunciable y obligatorio; y, d) La norma dé al particular al menos un margen de discrecionalidad, ya que de otra manera actuaría, más bien, como auxiliar del ente estatal. Ahora bien, el "Acuerdo

[111] Flores Pacheco, Moisés Israel, op. cit., p. 88

> mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996.", difundido a través del Diario Oficial de la Federación de dos de diciembre de dos mil quince y mediante el cual el citado instituto ejerció su facultad reguladora atiende a los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, atribuye diversas conductas a los concesionarios de telecomunicaciones, entre otras, en materia de localización geográfica de equipos de comunicación móvil y registro y control de las comunicaciones de sus usuarios, las cuales se traducen en obligaciones que deben asumir en auxilio de las autoridades de seguridad, procuración y administración de justicia; tan es así, que su incumplimiento provoca la imposición de sanciones, según se advierte de los artículos primero, quincuagésimo octavo y quincuagésimo noveno de los propios lineamientos, y que estos mismos indican que dichas conductas son una "colaboración". Luego, cuando los aludidos concesionarios actúan en términos de tales lineamientos, no lo hacen como autoridades responsables (ejecutoras), porque no obstante que su comportamiento al respecto deriva de una norma, es irrenunciable y afecta jurídicamente a los usuarios, no es una atribución, sino una obligación, la cual, en ese sentido, no es discrecional en grado alguno. De ahí que no obren con imperio en una relación de supra a subordinación frente a otros gobernados; por el contrario, lo hacen en colaboración con la autoridad, como auxiliares del ente estatal en sus funciones de orden público. Tesis: I.2o.A.E.34 A (10a.)[112]

Respecto a la siguiente jurisprudencia, la SCJN considero que era improcedente conceder el amparo frente a los artículos 189 y 190, fracciones I, III y IV, de la LFTR, en la cual se establecen obligaciones a los concesionarios de telecomunicaciones para proporcionar información y de contar permanentemente con los recursos humanos necesarios para cumplir con ese objetivo. La SCJN considero que los preceptos señalados son una herramienta para las autoridades para la prevención o persecución de delitos, y la suspensión les impediría a las autoridades contar con la información necesaria para la prevención o persecución de los delitos. A su vez que dichos artículo no son normas penales, y están orientadas a establecer reglas administrativas, dicha tesis a la letra dice lo siguiente:

> SUSPENSIÓN EN EL AMPARO INDIRECTO. ES IMPROCEDENTE CONCEDERLA CONTRA LOS EFECTOS Y CONSECUENCIAS DE LOS ARTÍCULOS 189 Y 190, FRACCIONES I, III Y IV, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN, EN

[112] Tesis I.2o.A.E.34 A, *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. IV, agosto de 2016, p. 2528.

> LOS QUE SE ESTABLECE LA OBLIGACIÓN DE LAS EMPRESAS CONCESIONARIAS EN LA PRIMERA DE ESAS MATERIAS DE EMPLEAR LA TECNOLOGÍA DESTINADA A LA GEOLOCALIZACIÓN, EN TIEMPO REAL, DE LOS EQUIPOS DE COMUNICACIÓN MÓVIL. En los artículos 189 y 190, fracciones I, III y IV, de la Ley Federal de Telecomunicaciones y Radiodifusión, publicada en el Diario Oficial de la Federación el 14 de julio de 2014, se establecen obligaciones genéricas a cargo de los concesionarios en la primera de esas materias de proporcionar la información requerida por las autoridades de seguridad, procuración y/o de administración de justicia, así como la obligación de contar permanentemente con los recursos humanos necesarios para cumplir con ese objetivo. Así, las prescripciones contenidas en los preceptos mencionados constituyen una herramienta adicional a las instancias administrativas y/o judiciales para la prevención o persecución de delitos, en razón de que a través del nuevo diseño impuesto a las empresas concesionarias de los servicios de telecomunicaciones podrá emplearse la tecnología destinada a la geolocalización, en tiempo real, de los equipos de comunicación móvil. Por tanto, es improcedente conceder la medida solicitada contra los efectos y consecuencias de esas disposiciones, ya que no se colmarían las exigencias contenidas en el artículo 128, fracción II, de la Ley de Amparo, dado que se impediría a las autoridades contar con la información necesaria para la prevención o persecución de los delitos. No es obstáculo a lo anterior que la normativa adjetiva penal expresamente prevea que tratándose de investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas, el procurador general de la República o los servidores públicos en quienes delegue la facultad puedan solicitar a los concesionarios o permisionarios del servicio de telecomunicaciones la localización geográfica, en tiempo real, de los equipos de comunicación móvil asociados a una línea, que se encuentren relacionados con una investigación, toda vez que el objetivo consignado en los artículos inicialmente citados es diverso al de las normas penales, dado que está orientado a establecer reglas administrativas a las empresas concesionarias. Tesis: I.1o.A.E.73 A (10a.)[113]

Como ya lo habíamos señalado, las solicitudes de acceso a los datos conservados o retenidos, debe realizarse conforme al artículo 16 constitucional, la inviolabilidad de las comunicaciones garantiza la reserva de todo proceso comunicativo, se protege el contenido de las comunicaciones, como son los siguientes:

a) los datos de identificación, pues éstos ofrecen información sobre las circunstancias en que se produce,
b) datos de la identidad de los interlocutores,

[113] Tesis I.1o.A.E.73 A (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. IV, octubre de 2016, p. 4101.

c) el origen y el destino de las llamadas telefónicas,
d) su duración y fecha.

La solicitud de acceso a los datos de tráfico retenidos por los concesionarios, debe realizarse exclusivamente por la autoridad judicial federal, mediante la debida fundamentación y motivar las causas legales, así como expresar a las personas de quienes solicitara los datos y el periodo de información.

> COMUNICACIONES PRIVADAS. LA SOLICITUD DE ACCESO A LOS DATOS DE TRÁFICO RETENIDOS POR LOS CONCESIONARIOS, QUE REFIERE EL ARTÍCULO 190, FRACCIÓN II, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN, DEBE REALIZARSE EN TÉRMINOS DEL ARTÍCULO 16 CONSTITUCIONAL Y SÓLO LA AUTORIDAD JUDICIAL PODRÁ AUTORIZAR LA ENTREGA DE LA INFORMACIÓN RESGUARDADA. El derecho a la inviolabilidad de las comunicaciones privadas previsto en el artículo 16, párrafos decimosegundo y decimotercero, de la Constitución Política de los Estados Unidos Mexicanos, tiene como objeto garantizar la reserva de todo proceso comunicativo, por lo que su ámbito de protección comprende tanto su contenido, como los datos de identificación, pues éstos ofrecen información sobre las circunstancias en que se produce, como son la identidad de los interlocutores, el origen y el destino de las llamadas telefónicas, su duración y fecha. En ese sentido, la solicitud de acceso a los datos de tráfico retenidos por los concesionarios para su entrega tanto en tiempo real como dentro de las 48 horas siguientes contadas a partir de la notificación de la solicitud, que refiere el artículo 190, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión, debe realizarse en términos del citado precepto constitucional, por lo que exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o el titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la entrega de la información resguardada, para lo cual se deberán fundar y motivar las causas legales de ésta, así como expresar las personas cuyos datos serán solicitados y el periodo por el cual se requiera la información. Tesis: 2a. XXXV/2016 (10a.)[114]

Si bien no corresponde a la conservación de datos, de igual forma se debió establecer para el caso de la retención de datos en la LFTR, con la finalidad de dar certidumbre a los gobernados, un listado de las autoridades que pueden hacer las solicitudes de conservación de datos, como son:

[114] Tesis 2a. XXXV/2016 (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. I, agosto de 2016, p. 776.

a) El Procurador General de la República, así como los Procuradores de las entidades federativas
b) Policía Federal; y,
c) La autoridad encargada de aplicar y coordinar directamente la instrumentación de la Ley de Seguridad Nacional

> LOCALIZACIÓN GEOGRÁFICA EN TIEMPO REAL DE LOS EQUIPOS DE COMUNICACIÓN MÓVIL PREVISTA EN EL ARTÍCULO 190, FRACCIÓN I, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN. AUTORIDADES COMPETENTES PARA SOLICITARLA Y PRESUPUESTOS QUE LA AUTORIZAN. Si bien la mencionada disposición legal hace referencia expresa a las "instancias de seguridad, procuración y administración de justicia" como las autoridades con que los concesionarios de telecomunicaciones y los autorizados deben colaborar en la localización geográfica en tiempo real de los equipos de comunicación móvil, lo cierto es que a fin de lograr un óptimo grado de certidumbre jurídica a los gobernados, así como enmarcar adecuadamente la actuación de las autoridades en esta materia, se considera que las autoridades a que se refiere la porción normativa aludida son: (I) el Procurador General de la República, así como los Procuradores de las entidades federativas y, en su caso, los servidores públicos en quienes deleguen esta facultad, en términos del artículo 21 de la Constitución Federal; (II) la Policía Federal, conforme a lo previsto en el artículo 8, fracción XXVIII, de la ley que la regula; y, (III) la autoridad encargada de aplicar y coordinar directamente la instrumentación de la Ley de Seguridad Nacional en los supuestos establecidos en su artículo 5. Así, sólo las autoridades referidas podrán solicitar la localización geográfica en tiempo real de los equipos de comunicación móvil cuando se presuma que existe un peligro para la vida o la integridad de las personas, lo que implica que dicha facultad no se circunscribe a un catálogo de delitos determinado, sino que encuentra su razón jurídica en la tutela de los derechos humanos a la vida y a la integridad personal, como valor supremo a cargo del Estado mexicano. Tesis: 2a. XLIV/2016 (10a.)[115]

4. Conflictos de interés

A partir de la reforma Constitucional en 2011, nuestro derecho incluye los tratados internacionales sobre derechos humanos que ahora se incorporan en el artículo primero constitucional[116].

[115] Tesis 2a. XLIV/2016 (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. II, agosto de 2016, p. 1305.
[116] Vázquez, Daniel, *Test de razonabilidad y derechos humanos: Instrucciones para armar,* México, Instituto de Investigaciones Jurídicas UNAM, 2016, p. 1

Para el autor Daniel Vázquez, lo primero que debemos distinguir es la distinción entre reglas y principios, así tenemos que la Constitución está formada por principios, de acuerdo con la SCJN se ha pronunciado que la Constitución está integrada por normas que establecen lo que es debido y se expresan en un mandato, por lo que la diferencia es la siguiente:

> La SCJN establece que la constitución está integrada por normas que pueden constituir principios o reglas. Se consideran que ambos son normas porque establecen lo que es debido y pueden ser expresadas en un mandato, un permiso o una prohibición. Lo que distingue a los principios de las reglas -sigue la corte- los primeros son disposiciones que ordenan que algo debe ser realizado en la mayor medida posible dentro de las posibilidades jurídicas y fácticas existentes; mientras que las reglas son mandatos que únicamente pueden o no ser cumplidos[117].

Si tenemos que dos reglas en conflicto, en ese caso podemos usar herramientas para dar una solución, hay mecanismos para declarar la invalidez, el mecanismo jerárquico determina una regla superior y otra inferior, otro ejemplo es el criterio de especialidad de una norma sobre una general, también el criterio de temporalidad de ley posterior deroga a la anterior. Pero cuando tenemos dos principios en colisión, las herramientas no funcionan y debemos hacer una actualización[118].

Debemos considerar que la ponderación no es una función propia o exclusiva de la actividad jurisdiccional, a veces la propia norma establecer reglas para su aplicación o que en determinados supuesto se pueden tomar en cuenta particularidades y justificar un trato diferente[119].

Los **test** deben ser considerados como herramientas argumentativas, en donde pueden variar los criterios que se utilicen dependiendo del objetivo del test, por

[117] Ibidem, p. 18
[118] Ibidem, p. 20
[119] Pahuamba Rosas, Baltazar (Coord), *Aplicación de los Derechos Humanos,* México, Novum, 2014, p. 148.

ejemplo para señalar lo que es razonable si se desea el núcleo de un derecho humano; o cuando se realiza una ponderación de derechos ejercidos por dos personas; otra situación se presenta si es válida y legal una restricción a un derecho humano para realizar un objetivo gubernamental, otra situación ocurre cuanto se presenta una revisión sobre una acción gubernamental y determinar si es acorde a los principios de progresividad y prohibición de regresión, etc. El caso que nos ocupa es determinar si una restricción al derecho a la privacidad con el fin de realizar una cuestión gubernamental se justifica plenamente.

Determinar si una restricción legítima de derechos es correcta, se utiliza el test de restricción de derechos. Para ello nos apoyamos en la idea de razonabilidad o proporcionalidad que se desarrolló a partir de la lógica y con la finalidad de determinar si una restricción de derechos como "la retención de las comunicaciones" es razonable o proporcional[120].

Los elementos para definir una legitimidad de la restricción son las siguientes:

Primero las restricciones de derechos humanos deben ser explicitas, en nuestro problema es explicita la obligación a los concesionarios de telecomunicaciones de conservar o retener los datos de las comunicaciones.

Un segundo elemento es el objetivo que persigue la restricción, cuando no se señala un objetivo específico esa ley o norma es ilegítima, retomando nuestro problema se ha en materia de retención de datos, el establecimiento de obligaciones a cargo de los concesionarios para proporcionar la información de las comunicaciones requeridas por las autoridades de seguridad, procuración y/o de administración de justicia. Esto constituye una herramienta adicional a las instancias administrativas y/o judiciales para la prevención o persecución de delitos.

[120] Vázquez, Daniel, op. cit., p. 55.

Los objetivos legítimos deben ser bastante amplios por lo tanto permite un margen de apreciación, como ejemplo se señalan los siguientes:

a) Se define como el conjunto de reglas sobre las cuales se erige una sociedad. La Corte IDH como las condiciones que aseguran el funcionamiento armónico y normal de las instituciones sobre la base de un sistema coherente de valores y principios.
b) Sobre seguridad nacional, hay consenso que la restricción debe operar bajo problemáticas que envuelven al Estado en su totalidad y no a un gobierno específico. Además, se considera que existe efectivamente un problema de seguridad nacional únicamente en aquellos casos donde existe una amenaza efectiva o el uso de la fuerza contra la integridad territorial o la independencia política de un Estado.
c) La seguridad pública se refiere a los peligros para la seguridad de las personas o de sus bienes.
d) El bien común fue desarrollado por el sistema interamericano como las condiciones de la vida social que permiten a los integrantes de la sociedad alcanzar el mayor grado de desarrollo personal y la mayor vigencia de valores democráticos[121].

Un tercer elemento exige que el objetivo además de legítimo, sino que sea necesario para la sociedad, se debe justificar la interferencia a los derechos humanos, en este caso se debe justificar plenamente la restricción a la privacidad y a la inviolabilidad de las comunicaciones.

Un cuarto elemento es la adecuación o idoneidad. Que el medio sea adecuado entre la restricción y el fin que se persigue. En todo momento se debe entender como la existencia de una causalidad entre la restricción como medios para obtener o llegar al objetivo legítimo que se busca.

[121] Ibidem, p. 58

Los criterios de idoneidad y necesidad, son conceptos diferentes, la *idoneidad* estudia la relación de los medios utilizados y el tipo de restricción con el objetivo legítimo de la restricción, y la *necesidad* analiza que esa restricción de derechos sea la única medida para conseguir los objetivos y no existan medidas alternativas.

El quinto elemento es la *necesidad* de la restricción para obtener al objetivo legítimo, necesitamos verificar que no existe una alternativa diferente que se obtiene con la restricción. En este punto no significa que sea útil para llegar al objetivo, sino que no sea posible la obtención del mismo resultado por otros medios[122].

Un sexto elemento es que la restricción sea *proporcional*, como lo hemos mencionado no es suficiente el conseguir el objetivo, sino que debemos encontrar la forma menos gravosa o la menor afectación posible al goce o ejercicio de un derecho, eso significa que existe una forma menos gravosa, debemos aplicar la nueva alternativa, la proporcionalidad se trata de una medición en torno al nivel o grado de restricción.

Como se ha planteado en capítulos anteriores, la proporcionalidad no debe ser exagerada para que no afecte a las personas en sus derechos en forma excesiva, una carga desmedida o injustificada.

El séptimo criterio es que la medida no sea una *anulación de derechos*, es decir que la implementación de la restricción continúe respetando los contenidos esenciales de la norma. Si la existencia de las limitaciones termina por negar el derecho no encontramos ante una anulación de derechos, por ejemplo, realizar restricciones a la libertad de expresión, no deben poner en peligro la existencia del mismo derecho.

Consideramos que con la retención de las comunicaciones se violan varios criterios en la restricción de derechos, uno de ellos es que la medida implementada no es proporcional porque no es necesario que se obligue a los concesionarios a

[122] Ibidem, p. 63

almacenar sin motivos las comunicaciones de todos los usuarios. Aun de quienes no tengan motivo o causa que se relacione con el supuesto objetivo que es la prevención y prosecución de los delitos.

Otro de los criterios que se violan es la anulación de un derecho, se supone la existencia de un derecho a la inviolabilidad de las comunicaciones, sin embargo, ahora en con la retención de datos en forma general, puede el Estado intervenir de forma discrecional a cualquier usuario, y las autoridades pueden obtener la información de cualquier usuario, con el simple hecho de decir que necesita la información por cuestiones de seguridad. Definitivamente el derecho a la inviolabilidad desaparece si desde su origen ya está siendo almacenada hasta por un lapso de 2 años.

De acuerdo con la Suprema Corte de Justicia de la Nación, el test de restricción debe seguir los siguientes elementos:

> GARANTÍAS INDIVIDUALES. EL DESARROLLO DE SUS LÍMITES Y LA REGULACIÓN DE SUS POSIBLES CONFLICTOS POR PARTE DEL LEGISLADOR DEBE RESPETAR LOS PRINCIPIOS DE RAZONABILIDAD Y PROPORCIONALIDAD JURÍDICA**.**
> De los criterios emitidos por la Suprema Corte de Justicia de la Nación se advierte que el cumplimiento de los principios de razonabilidad y proporcionalidad implica que al fijar el alcance de una garantía individual por parte del legislador debe: a) perseguir una finalidad constitucionalmente legítima; b) ser adecuada, idónea, apta y susceptible de alcanzar el fin perseguido; c) ser necesaria, es decir, suficiente para lograr dicha finalidad, de tal forma que no implique una carga desmedida, excesiva o injustificada para el gobernado; y, d) estar justificada en razones constitucionales. Lo anterior conforme al principio de legalidad, de acuerdo con el cual el legislador no puede actuar en exceso de poder ni arbitrariamente en perjuicio de los gobernados. Tesis: Tesis P./J. 130/2007 (9a.)[123]

[123] Tesis P./J. 130/2007, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXVI, diciembre de 2007, p. 8.

Consideramos que la conservación de datos afecta una serie de derechos como la privacidad, la intimidad, derecho a la protección de datos personales y limita la libertad de expresión, que tienen un alto nivel constitucional todos ellos considerados derechos humanos.

Debido a la seria afectación de estos derechos fundamentales, no creemos que la autoridad cuente con razones materiales ciertas y confiables para demostrar el beneficio que tal restricción al derecho a la privacidad y protección a los datos personales quede plenamente acreditado por la autoridad, como veremos en la parte de estadísticas solo un porcentaje mínimo ha sido utilizado para la finalidad que fue creada.

5. Estadísticas

En el año 2013 en México teníamos un aproximado de 45.1 millones de cibernautas de los cuales 15 millones eran menor de edad con un alto promedio de uso de 5 horas diarias mediante cualquier dispositivo electrónico[124]. El para dimensionar el avance constante en 2011 sólo el 7% de la población podía acceder a Internet por medio de su teléfono móvil; para mediados de 2013, 23 de cada 100 habitantes y para finales de 2016, el 61% de la población contaba con Internet de Banda Ancha Móvil en su dispositivo[125].

Si bien es cierto que contamos con mejor internet y servicio de telecomunicaciones, no se informa sobre las formas de investigación y retención de datos, no dan un informe claro sobre el número de geolocalizaciones realizada y solicitudes de retención de datos, en la cual se puedan obtener resultados sobre las medidas de restricción.

---

[124] Luna Pla, Issa (Coord), *Estudios aplicados sobre la libertad de expresión y el derecho a la información,* México, Instituto de Investigaciones Jurídica, UNAM, 2014, p. 83

[125] Instituto Federal de Telecomunicaciones. Las Telecomunicaciones a 3½ años de la Reforma Constitucional en México, http://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/a3anosreforma-acc1.pdf

En México, los riesgos al uso de internet van en aumento, en la *Encuesta nacional sobre disponibilidad y uso de las tecnologías de la información en los hogares* de 2015, se señala que 55,735,713 millones de personas somos usuarias de computadoras que representa el 51.3%, un total de 62,448,892 usuarios de internet con un porcentaje del 57.4% del total de la población y por último 77,711,203 que utilizan telefonía móvil celular, lo cual significa un 77.5% del total de la población[126], lo cual incluye los servicios de navegación en internet[127].

a) Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2016

De acuerdo a la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2016, el objetivo era conocer las experiencias, actitudes y percepciones que influyen en el ejercicio de los derechos de acceso a la información y protección de datos personales, así como el grado de conocimiento sobre la legislación y las instituciones encargadas de garantizarlo[128].

Dentro de las preguntas más interesantes encontramos si conocen existencia de una Ley encargada de garantizar la protección de datos personales

- Población de 18 años y más que habita en áreas urbanas de cien mil habitantes y más que conoce o ha escuchado sobre la existencia de una Ley encargada de garantizar la protección de datos personales por regiones, según su conocimiento sobre la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[126] INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, 2015, disponible en: http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2015/
[127] Sánchez Hernández, Néstor Mauricio, op. cit., 55
[128] INEGI, Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAID) 2016, disponible en: http://www.beta.inegi.org.mx/proyectos/enchogares/especiales/enaid/2016/

Región	Población de 18 años y más que conoce o ha escuchado una Ley[1]	Conocimiento sobre la existencia de una Ley encargada de garantizar la protección de datos personales					
		Ley Federal de Protección de Datos Personales en Posesión de los Particulares		Otro		No recuerda el nombre	
		Absolutos	Relativos	Absolutos	Relativos	Absolutos	Relativos
Estados Unidos Mexicanos	**25 841 675**	**2 575 558**	**10.0**	**1 323 018**	**5.1**	**19 522 573**	**75.5**
Región Centro[2]	11 415 188	1 401 469	12.3	717 365	6.3	9 009 148	78.9
Región Centro Occidente[3]	4 882 556	436 872	8.9	253 875	5.2	3 468 389	71.0
Región Norte[4]	7 237 714	502 126	6.9	284 576	3.9	5 428 315	75.0
Región Sureste[5]	2 306 217	235 091	10.2	67 202	2.9	1 616 721	70.1

De acuerdo a las cifras solo el 10% conoce el nombre de la LFPDPPP, asimismo, solo el 55% sabe de la existencia de la LFPDPPP, todo representa un gran problema porque si la sociedad no conoce el derecho a la protección de sus datos personales, difícilmente podemos exigir que las empresas cumplan con su obligación de haber notificado el cambio de las finalidades y la posibilidad de realizar transferencias a las autoridades sin nuestro consentimiento o autorización.

Asimismo, no podremos exigir que no existe una relación entre el servicio prestado que es la comunicación y la retención de nuestros datos por el plazo de dos años.

Región	Población de 18 años y más[1]	Conoce o ha escuchado una Ley[2]	
		Absolutos	Relativos
Estados Unidos Mexicanos	**46 316 127**	**25 841 675**	**55.8**
Región Centro[3]	20 242 016	11 415 188	56.4
Región Centro Occidente[4]	8 663 259	4 882 556	56.4
Región Norte[5]	12 608 860	7 237 714	57.4
Región Sureste[6]	4 801 992	2 306 217	48.0

Otra pregunta sobre la percepción de la protección de datos se refiere al condicionamiento para la prestación del servicio, es decir si deseamos utilizar un servicio de telefonía celular, debemos aceptar las condiciones.

- Población de 18 años y más que habita en áreas urbanas de cien mil habitantes y más a la que le dieron a conocer un aviso de privacidad y lo leyó por región, según condicionamiento de la prestación de un servicio a cambio de firmar o aceptar algún aviso de privacidad

Región	Población de 18 años y más[1]	Desconocimiento sobre un aviso de privacidad o conocimiento y lectura del mismo[2]		Condicionamiento de la prestación de un servicio			
				Sí		No	
		Absolutos	Relativos	Absolutos	Relativos	Absolutos	Relativos
Estados Unidos Mexicanos	**46 316 127**	**41 030 561**	**88.6**	**2 992 654**	**7.3**	**37 820 644**	**92.2**
Región Centro[3]	20 242 016	18 261 175	90.2	1 183 040	6.5	16 969 180	92.9
Región Centro Occidente[4]	8 663 259	7 647 257	88.3	636 241	8.3	6 978 871	91.3
Región Norte[5]	12 608 860	10 852 528	86.1	941 592	8.7	9 858 293	90.8
Región Sureste[6]	4 801 992	4 269 601	88.9	231 781	5.4	4 014 300	94.0

b) Estadísticas Red en Defensa de los Derechos Digitales

De acuerdo a la asociación Red en Defensa de los Derechos Digitales, a través de diversas solicitudes de información ante las autoridades obtuvieron que datos sobre los requerimientos de acceso a datos conservados, para ello en 2014 se realizaron

18111 y para el año 2015 fueron 14129 los requerimientos a concesionarios de telecomunicaciones.

Lo grave sobre los requerimientos en el año 2014 es que solamente el 1.09% se realizó a través de autorización judicial esto significa que la mayoría de los requerimientos no fueron realizados conforme a lo establecido en la Constitución[129]*. Los datos indican que el número de autoridades que han realizado solicitudes de acceso a los datos retenidos ha aumentado a partir de 2014.*

De acuerdo a los informes semestrales enviados por las empresas de telecomunicaciones al IFETEL, en el primer semestre de 2016, más de 46 autoridades solicitaron requerimientos de acceso a la conservación de datos, información que obtuvo la asociación a través de solicitudes de acceso.

Un dato relevante en la eficacia en los requerimientos, puesto que solo el 8.73% de las averiguaciones previas en las que se utilizado alguna medida de vigilancia entre 2013 y 2015 se ha ejercido acción penal. Lo cual significa que casi el 90% de las personas vigiladas no han sido procesadas o sido acusadas de ningún delito ante un juez.

Con esto podemos darnos cuenta que no es utilizada la retención de datos para los fines o el objetivo para el cual fue creada que es la prevención y prosecución de los delitos, es preocupante que las autoridades investigadoras vigilen a personas y no sean procesadas. Y en el peor de los casos sean vigiladas personas contra las cuales no existe evidencia o indicios de su participación en la comisión de un delito[130].

[129] Red en Defensa de los Derechos Digitales, op. cit*. p.*52
[130] Ibidem, p. 74

CAPÍTULO CUARTO. LÍMITES A LA CONSERVACIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS CONCESIONARIOS DE TELECOMUNICACIONES

1. Limitaciones a la vigilancia

Los requerimientos sobre el acceso a los datos retenidos, deben tener mecanismo de control, dichos requerimientos deben ser utilizados de exclusivamente para el objetivo legítimo por el cual fue creado, que es la prevención de delitos y procuración de justicia, en ese sentido se debe respetar el principio de proporcionalidad, no deben realizarse de forma generalizada.

En otras palabras, la afectación de un principio deber ser directamente proporcional a la importancia de que el otro principio sea respetado[131].

En la protección de datos personales, la Comisión Interamericana ha señalado que los Estados deben prohibir el uso de los datos cuando sean contrarios a los derechos humanos, haciendo énfasis en la aplicación del criterio de necesidad y proporcionalidad, así como la implementación de un efectivo sistema de supervisión[132].

El criterio de *necesidad*, implica al momento de aplicar una restricción a un derecho que se debe establecer claramente la obligación de efectuar dicha limitación, es decir, que tal objetivo legítimo e imperativo no pueda alcanzarse razonablemente por un medio menos restrictivo de los derechos humanos.

También implica que no debe limitarse más allá de lo estrictamente indispensable, sugiere que el medio restrictivo sea en realidad el medio menos gravoso disponible para “proteger los bienes jurídicos fundamentales (protegidos) de los ataques más

[131] Pahuamba Rosas, Baltazar, op. cit., p. 140.
[132] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Libertad de Expresión e Internet,* op. cit., p. 66

graves que los dañen o pongan en peligro", pues lo contrario llevaría al ejercicio abusivo del poder del Estado. Dicho de otra forma debe escogerse la que restrinja en menor escala el derecho protegido[133].

En cuanto a la *proporcionalidad*, debe ajustarse estrechamente al logro de ese objetivo, interfiriendo en la menor medida posible con el ejercicio legítimo de tal libertad.

De acuerdo a las Corte Interamericana, para establecer la proporcionalidad, se deben evaluar tres factores:

(i) el grado de afectación del derecho contrario- grave, intermedia, moderada-;
(ii) la importancia de satisfacer el derecho contrario; y
(iii) si la satisfacción del derecho contrario justifica la restricción de la libertad de expresión. No hay respuestas *a priori* ni fórmulas de aplicación general en este ámbito: el resultado de la ponderación variará en cada caso, en algunos casos privilegiando la libertad de expresión, en otros el derecho contrario. Si la responsabilidad ulterior aplicada en un caso concreto resulta desproporcionada o no se ajusta al interés de la justicia, hay una violación del artículo 13.2 de la Convención Americana[134].

En este capítulo señalamos las limitaciones a la retención de datos para las autoridades, y porque debería modificarse el actual marco normativo, la primera limitación analizar es la existencia de una Ley previa a una restricción a un derecho humano.

---

[133] *Cfr.* Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos, *Marco Jurídico Interamericano sobre el Derecho a la Libertad de Expresión*. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/MARCO%20JURIDICO%20INTERAMERICANO%20DEL%20DERECHO%20A%20LA%20LIBERTAD%20DE%20EXPRESION%20ESP%20FINAL%20portada.doc.pdf, consultado el 27 de noviembre de 2017, p. 30
[134] Ibidem, p. 30 y 31

a) Ley Previa

De acuerdo al Sistema Interamericano, para que la existencia de una limitación a los derechos, deben estar establecido en forma previa en forma precisa y clara en una ley.

La intención era que la LFTR fuera consecuencia de un acto legislativo en el que se definieran las casusas precisas y las condiciones para que el Estado pudiera intervenir las comunicaciones o solicitar los datos conservados[135].

La Corte Interamericana ha señalado que la intercepción de las comunicaciones no solo debe estar establecido con claridad y precisión sino además solo podrá autorizarse por un juez. Así como, señalar el alcance y duración de las medidas de vigilancia; sin olvidar los hechos para justificar tales acciones y las dejar claramente establecido que autoridades son competentes para autorizarlas, llevarlas a cabo y supervisarlas. La ley debe establecer la forma de subsanar los abusos cometidos por las autoridades en el abuso en el ejercicio de sus facultades[136].

Las facultades del Estado para una vigilancia deben establecerse de manera **clara, precisa y detallada en una ley**. Es esencial que las personas conozcan las causas por las cuales puedes ser vigiladas, asimismo conocer que autoridades y los procedimientos que deben observarse para evitar abusos por parte de las autoridades[137].

b) Proporcionalidad y necesidad

Como lo hemos venido señalando los principios de necesidad y proporcionalidad, las medidas de vigilancia solamente pueden ser legitimas para lograr el objetivo,

[135]Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Libertad de Expresión e Internet*, op. cit., p. 66, pp. 74 y 75
[136] Ibidem, p. 76
[137] Red en Defensa de los Derechos Digitales, op. cit., p. 8

cuando las afectaciones a la privacidad no son exageradas o desmedidas frente las ventajas de la vigilancia.

Por eso coincidimos que al constituir una afectación generalizada y de forma indiscriminada no puede considerarse una medida legitima por parte del Estado, la intervención o retención de datos debe ser focalizada y previamente justificada a un caso concreto.

La SCJN ha señalado que para cumplir con el principio de proporcionalidad en las restricciones de un derecho fundamental deben cumplir con los siguientes requisitos:

(i) que la intervención legislativa persiga un fin constitucionalmente válido;

(ii) que la medida resulte idónea para satisfacer en alguna medida su propósito constitucional;

(iii) que no existan medidas alternativas igualmente idóneas para lograr dicho fin, pero menos lesivas para el derecho fundamental; y,

(iv) que el grado de realización del fin perseguido sea mayor al grado de afectación provocado al derecho fundamental por la medida impugnada. En este contexto, si la medida legislativa no supera el test de proporcionalidad, el derecho fundamental preservará su contenido inicial o prima facie.[138]

[138] TEST DE PROPORCIONALIDAD. METODOLOGÍA PARA ANALIZAR MEDIDAS LEGISLATIVAS QUE INTERVENGAN CON UN DERECHO FUNDAMENTAL.
El examen de la constitucionalidad de una medida legislativa debe realizarse a través de un análisis en dos etapas. En una primera etapa, debe determinarse si la norma impugnada incide en el alcance o contenido inicial del derecho en cuestión. Dicho, en otros términos, debe establecerse si la medida legislativa impugnada efectivamente limita al derecho fundamental. De esta manera, en esta primera fase corresponde precisar cuáles son las conductas cubiertas prima facie o inicialmente por el derecho. Una vez hecho lo anterior, debe decidirse si la norma impugnada tiene algún efecto sobre dicha conducta; esto es, si incide en el ámbito de protección prima facie del derecho aludido. Si la conclusión es negativa, el examen debe terminar en esta etapa con la declaración de que la medida legislativa impugnada es constitucional. En cambio, si la conclusión es positiva, debe pasarse a otro nivel de análisis. En esta segunda fase, debe examinarse si en el caso concreto existe una justificación constitucional para que la medida legislativa reduzca o limite la extensión de la protección que otorga inicialmente el derecho. Al respecto, es necesario tener presente que los derechos y sus respectivos límites operan como principios, de tal manera que las relaciones entre el derecho y sus límites encierran una colisión que debe resolverse con ayuda de un método específico denominado test de proporcionalidad. En este orden de ideas, para que las intervenciones que se

De acuerdo a lo anterior, no consideramos que la conservación de datos sea constitucionalmente valida ya que existen medidas alternativas para la prosecución de los delitos, el cuidado y preservación de la seguridad nacional o seguridad pública. Asimismo, el grado de afectación al derecho a la privacidad no debe realizarse en forma generalizada, existe la posibilidad de legislar idóneas o menos lesivas, como ejemplo señalar que solo se realizara la conservación de datos por un máximo de 6 meses.

Por lo que se refiere a la *necesidad* la SCJN ha señalado que significa corroborar, en primer lugar, si existen otros medios igualmente idóneos para lograr los fines que se persiguen y, en segundo lugar, determinar si estas alternativas intervienen con menor intensidad el derecho fundamental afectado. Lo anterior supone hacer un catálogo de medidas alternativas y determinar el grado de idoneidad de éstas, es decir, evaluar su nivel de eficacia, rapidez, probabilidad o afectación material de su objeto[139]

realizan a algún derecho fundamental sean constitucionales debe corroborarse lo siguiente: (i) que la intervención legislativa persiga un fin constitucionalmente válido; (ii) que la medida resulte idónea para satisfacer en alguna medida su propósito constitucional; (iii) que no existan medidas alternativas igualmente idóneas para lograr dicho fin, pero menos lesivas para el derecho fundamental; y, (iv) que el grado de realización del fin perseguido sea mayor al grado de afectación provocado al derecho fundamental por la medida impugnada. En este contexto, si la medida legislativa no supera el test de proporcionalidad, el derecho fundamental preservará su contenido inicial o prima facie. En cambio, si la ley que limita al derecho se encuentra justificada a la luz del test de proporcionalidad, el contenido definitivo o resultante del derecho será más reducido que el contenido inicial del mismo. Tesis 1a. CCLXIII/2016 (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima Época, t. II, noviembre de 2016, p. 915.

[139] TERCERA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA NECESIDAD DE LA MEDIDA LEGISLATIVA.
Para que resulten constitucionales las intervenciones que se realicen a algún derecho fundamental, éstas deben superar un test de proporcionalidad en sentido amplio. Lo anterior implica que la medida legislativa debe perseguir una finalidad constitucionalmente válida, lograr en algún grado la consecución de su fin y no limitar de manera innecesaria y desproporcionada el derecho fundamental en cuestión. Así, una vez que se ha constatado un fin válido constitucionalmente y la idoneidad de la ley, corresponde analizar si la misma es necesaria o si, por el contrario, existen medidas alternativas que también sean idóneas pero que afecten en menor grado el derecho fundamental. De esta manera, el examen de necesidad implica corroborar, en primer lugar, si existen otros medios igualmente idóneos para lograr los fines que se persiguen y, en segundo lugar, determinar si estas alternativas intervienen con menor intensidad el derecho fundamental afectado. Lo anterior supone hacer un catálogo de medidas alternativas y determinar el grado de idoneidad de éstas, es decir, evaluar su nivel de eficacia, rapidez, probabilidad o afectación material de su objeto. De esta manera, la búsqueda de medios alternativos podría ser interminable y requerir al juez constitucional imaginarse y analizar todas las alternativas posibles. No obstante, dicho escrutinio puede acotarse

Los métodos de vigilancia no deben representar un problema para la seguridad y la privacidad de forma generalizada, no consideramos correcto que los proveedores de telecomunicaciones se encuentren obligados a diseñar e implementar sistemas que almacenen información con el objetivo de facilitar la vigilancia al Estado[140].

En relación a la protección de datos, no existe una notificación al afectado sobre las medidas de vigilancia que fueron implementadas en su persona. Por ello no hay una forma de saber si fueron vigiladas y, en su caso, estar en posibilidad de acudir a los mecanismos jurídicos o las instancias que se considere frente a posibles abusos[141].

Los proveedores de servicios no deberían estar obligados a revelar datos sobre sus usuarios cuando la finalidad era una prestación de servicio, los concesionarios se exceden en su finalidad, el Estado ha sido quien los obliga por disposición de Ley, pero consideramos que debe hacerlo en circunstancias limitadas, cuidando la privacidad de las comunicaciones. Por último, la retención de datos debe realizarse a usuarios específicos y conocidos no a gran escala a las comunicaciones por internet[142].

2. Órgano revisor a las solicitudes de vigilancia

No existe un órgano especializado sobre el control de las solicitudes de datos retenidos, en materia de transparencia el artículo 70 fracción XLVII la Ley General de Transparencia y Acceso a la Información señala como obligaciones comunes y

ponderando aquellas medidas que el legislador consideró adecuadas para situaciones similares, o bien las alternativas que en el derecho comparado se han diseñado para regular el mismo fenómeno. Así, de encontrarse alguna medida alternativa que sea igualmente idónea para proteger el fin constitucional y que a su vez intervenga con menor intensidad al derecho, deberá concluirse que la medida elegida por el legislador es inconstitucional. En caso contrario, deberá pasarse a la cuarta y última etapa del escrutinio: la proporcionalidad en sentido estricto. Tesis 1a. CCLXX/2016 (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima Época, t. II, noviembre de 2016, p. 914.

[140] Red en Defensa de los Derechos Digitales, op. cit., p. 10

[141] Ibidem, p. 14

[142] Aol, et. al Reform Government Surveillance (*Reforma de la Vigilancia Gubernamental*), disponible en: https://www.reformgovernmentsurveillance.com/

con efectos estadísticos, el listado de solicitudes a los concesionarios de telecomunicaciones sobre la intervención de comunicaciones privadas, el accesos a los registros y en su caso la locación geográfica en tiempo real, así como la temporalidad, fundamento legal y mención de la autorización judicial. En este caso puede haber a una sanción o multa al sujeto obligado, sin embargo, el INAI, no es autoridad supervisora sobre el uso, destino de las solicitudes de intervención de las comunicaciones.

La fracción XLVII de este artículo obliga a las autoridades facultadas para llevar a cabo medidas de vigilancia como la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, a publicar datos sobre las solicitudes que realizan:

> Artículo 70.
> XLVII. Para efectos estadísticos, el listado de solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de Internet para la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, que contenga exclusivamente el objeto, el alcance temporal y los fundamentos legales del requerimiento, así como, en su caso, la mención de que cuenta con la autorización judicial correspondiente, y […]

No contamos con mecanismos de supervisión sobre las autoridades que realizan solicitudes de acceso a los datos retenidos, y tampoco existe una como se ha planteado una obligación de notificar a quienes han sido objeto de vigilancia.

El principal problema radica en el desconocimiento de la sociedad sobre la interferencia del Estado en nuestro derecho a la privacidad y a la intervención de las comunicaciones. La falta del conocimiento o la falta de notificación a quienes han sido vigilados es desconocida, como lo hemos señalado solo un 10% de todas las solicitudes que se han realizado culmina en ejercicio de la acción penal, ello significa que se ha realizado un ejercicio abusivo en la retención de datos. Por ello

es necesario una instancia que vigile para evitar abusos, sanciones por parte de las autoridades competentes.

Típicamente se ha reconocido que esa función de control le corresponde a una autoridad judicial, la cual debe ponderar, de manera previa o inmediata, la legitimidad de cualquier medida de vigilancia encubierta y su estricto apego a la ley y a los principios de finalidad legítima, idoneidad, necesidad y proporcionalidad[143].

En este sentido la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos ha señalado que debe ser idónea y ser proporcional con el derecho que se pretende proteger[144].

Es necesario y se ha recomendado en la resolución "El derecho a la privacidad en la era digital", por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013, que los Estados deben establecer mecanismo de supervisión independiente y efectivos para asegura la transparencia y la rendición de cuentas sobre las actividades de vigilancia y recopilación de datos personales que realiza el Estado[145].

Necesitamos una instancia que proteja a las personas y conozcan sobre las leyes, reglamentaciones y formas de vigilancia secreta existente, conocer además los procedimientos para la autorización, objetivos, asimismo se encargue el tratamiento de la información sobre el intercambio, transferencias almacenamiento y garanticen la eliminación y destrucción[146].

---

[143] Red en Defensa de los Derechos Digitales, op. cit., p. 11

[144] "Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover".
(CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 165)

[145] Red en Defensa de los Derechos Digitales, op. cit., p. 13

[146] Ibidem,, p. 26

Autoridad de Control de la Unión Europea

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Es rescatable el artículo 46 en cuanto a las funciones que debe tener la autoridad de control, entre otras la función de supervisar y hacer cumplir las disposiciones, todo ello en específico sobre los datos personales.

Se deber encargar de la promoción de los riesgos relativos al tratamiento de los datos personales, asesorar, sobre de las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento; promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones.

Proporcionar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud de la presente Directiva y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados.

Atender las reclamaciones presentadas por un interesado o un organismo, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable,

Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de velar por la coherencia en la aplicación y ejecución de la presente Directiva.

Hacer un análisis y seguimiento de asunto que sean de relevancia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación[147].

Con el establecimiento de un organismo de supervisión, es posible que un funcionario realizase mejor su trabajo cuando existen controles[148]. Sin embargo, debe ser el problema es una verdadera autonomía del órgano supervisor.

3. Seguridad de los Datos Personales

Una de las obligaciones más importantes que tienen los concesionarios como responsables en el tratamiento de los datos personales, es la proteger los datos que en este caso recoge, trata y/o almacena. Como ya lo señalamos es uno de los deberes que se encuentran en la LFPDPPP.

La seguridad de los datos personales representa un grave problema, en la actualidad nuestra información no solo se encuentra en entes privados también en muchas bases de datos públicas, las cuales son almacenados para su tratamiento en muchas ocasiones tienen información que no tiene relación con la actividad que se lleva a cabo.

Por ello la información en poder de los concesionarios de telecomunicaciones para su tratamiento debe ser protegida contra cualquier vulneración, sea en el uso, en el almacenamiento, en la transferencia, en su recopilación, etc. Inclusive medidas físicas como son impedir el acceso por personas o instituciones públicas o privadas no autorizadas. La importancia de datos consiste en otorgar una enorme capacidad de fiscalización y control de la ciudadanía[149].

[147] Directiva (UE) 2016/680 op. cit.
[148] Carbonell, Miguel, *El ABC de los derechos humanos y del control de convencionalidad*, México, Porrúa, 2015, p. 137
[149] Ponce Baéz, Gabriela y García Tinajero, Leonel, op. cit., p. 76

Los riesgos pueden ser consecuencia de la actividad humana o casos fortuitos, accidentes, sin embargo, el responsable en este caso los concesionarios de telecomunicaciones deben adoptar las medidas adecuadas y necesarias para garantizar la protección de los datos contra cualquier vulneración, sea destrucción, perdida, acceso, difusión, etc.[150]

Es importante hacer mención que al momento en que las autoridades obtienen la información adquieren el carácter de responsables en el manejo tratamiento de los datos personales. Por ello deben cumplir con toda la normativa en materia de protección de datos personales la cual se homologo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual fue publicada en el Diario Oficial de la Federación el 27 de enero de 2017.

Por ello el responsable tiene el deber de adoptar las medidas físicas, técnicas y organizativas para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, dada la naturaleza de los datos almacenados[151].

a) La Directiva 2002/58/CE del Parlamento Europeo

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (Directiva sobre la privacidad de las comunicaciones electrónicas)

[150] Miguel Pérez, Julio César, *Protección de datos y seguridad de la información*, Madrid, España, Ra-Ma, 2015, p. 124
[151] Idem

Tiene como objetivo garantizar un nivel equivalente de protección de las libertades y derechos fundamentales, entre ellos la confidencialidad y el derecho a la intimidad, en el tratamiento de los datos personales en el sector de las comunicaciones[152].

Se establecen como objetivos evitar el acceso no autorizado a las comunicaciones para garantizar la confidencialidad, la prohibición del almacenamiento por terceros sin el consentimiento de los usuarios la finalidad es la transmisión de red de comunicaciones y se debe evitar que la información sea almacenada más tiempo del previsto para la gestión de tráfico. Y solo podrán establecer limitaciones por cuestiones de seguridad nacional, defensa, seguridad pública, persecución de delitos, para ello los Estados deberán justificar el establecimiento de un plazo.

Los Estados deben tener medidas técnicas para preservar la seguridad de sus servicios. Principalmente garantizar la confidencialidad de las comunicaciones y de los datos de tráfico, por ello se prohíbe la grabación, escucha, almacenamiento y otros tipos de vigilancia de las comunicaciones o de los datos de tráfico sin el consentimiento de los usuarios.

Una de las formas para proteger el derecho a la intimidad consiste en tomar medidas para la restricción de la identificación en línea de origen y de la línea conectada. El usuario puede otorgar su consentimiento para el trato de sus datos y tendrá la posibilidad de retirar su consentimiento al respecto[153].

De acuerdo con el artículo 15 de la Directiva 2002/58/CE, los Estado pueden exceptuar las disposiciones siempre y cuando dicha limitación constituya una medida necesaria proporcionada y apropiada para proteger la seguridad nacional,

[152] La Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. http://ec.europa.eu/justice/data-protection/law/files/recast_20091219_es.pdf

[153] Navarro Isla, Jorge, op. cit., p. 56

la defensa, la seguridad pública o la utilización no autorizada de comunicaciones electrónicas.

4. Eliminación de los datos personales conservados

Una de las causas que determinan que la retención de datos no es correcta, es la falta de garantizar a los usuarios que al término que establece la LFTR es la eliminación de los datos personales tratados. Actualmente no se cuenta con un procedimiento, por lo que no se asegura la correcta eliminación de las comunicaciones.

Como se señaló una de las finalidades de las medidas de seguridad es evitar la alteración, pérdida o acceso no autorizado, por ello tenemos dos recomendaciones:

- Una recomendación es clasificar la información para saber cuándo debe ser destruida, y tener información que solo es de carácter temporal.
- Otra recomendación es utilizar el menor tiempo posible la información, de acuerdo con el principio de calidad.

De acuerdo con la LFPDPPP, el plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, y tampoco deben exceder cuando se requiere para el cumplimiento de los siguientes supuestos:

a) Las disposiciones legales aplicables en materia del asunto de que se trate;
b) Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y
c) El periodo de bloqueo.

5. Garantías a la Libertad de Expresión por parte del Estado

En las relaciones sociales nos encontramos con la protección de derechos humanos cuando nos encontramos en un estado de indefensión frente a quienes tienen mayor poder, así tenemos como ejemplo los derechos humanos a la víctima de un delito, de los trabajares frente al patrón o todas las personas ante los gobernantes[154]. Dicho de otra forma, los derechos humanos son límites frente al poder de decisión de una mayoría que ocupe temporalmente los poderes públicos representativos[155].

La Relatoría Especial para Libertad de Expresión, considera que en los casos en que se justifique en la seguridad nacional para vigilar la correspondencia y los datos personales, la ley debe limitar el ejercicio de interpretaciones discrecionales, debe fijar claramente los criterios para que las limitaciones sean legítimas. La Relatoría Especial señala que el concepto de seguridad nacional debe ser definido desde una perspectiva democrática[156].

[154] Carbonell, Miguel, *El ABC de los derechos humanos y del control de convencionalidad*, México, Porrúa, 2015, p. 9
[155] Ibidem, p. 11
[156] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Libertad de Expresión e Internet*, op. cit. p. 78

CONCLUSIONES

Cuando se pretenda utilizar la seguridad nacional como justificación para vigilar la conservación de los datos personales, la ley debe limitar el ejercicio de interpretaciones discrecionales, por ello se debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de excepciones a la privacidad son legítimas.

No se respetaron las recomendaciones en derecho internacional como son: otorgar facultades a una instancia como el INAI para que proteja a las personas y conozcan sobre la supervisión y sanción en las solicitudes de acceso a los datos conservados; no se realizó un test de proporcionalidad y necesidad sobre el derecho a la privacidad, la protección de datos personales frente a la seguridad nacional sobre la cual se justifica la limitación a estos derechos fundamentales.

De acuerdo a lo señalado desarrollado en el presente trabajo, no consideramos justificable el plazo de conservación de los datos personales de hasta 24 meses, no es justificable que nuestros datos se conserven sin que existe un procedimiento en nuestra contra por presuntos responsables en la comisión de un delito, al igual que millones de usuarios implica una violación a la presunción de inocencia que establece el artículo 20, apartado B), fracción de la CPEUM.

De acuerdo a las estadísticas, se observa que las autoridades judiciales aumentaron en el número de solicitudes y en el año 2014 solo el 1.09% de las solicitudes fue concluida de forma satisfactoria, es por ello que consideramos que es un abuso que las autoridades investigadoras vigilan a personas y sea con los supuestos fines de seguridad, por otra parte, es más preocupante que personas sean vigiladas cuando no existen indicios de haber participado en la comisión de un delito.

Con la retención de datos la facultad para la conservación de datos se ha ampliado sin embargo no se han implementado controles sobre el su uso. La *primera limitante*

que consideramos importante en evitar que se realice la retención de datos en forma generalizada y sea utilizada solo en casos específicos en los cuales se presuma fehacientemente actos o hechos constitutivos de delitos.

Una *segunda limitación* que se debe establecer es cambiar el plazo excesivo de conservación de datos de hasta dos años lo cual representa una medida excesiva, sin embargo, aún continúa siendo excesiva que la disposición del artículo 190 fracción II sea generalizada. Pero debido a la existencia de casos reales de seguridad nacional y seguridad pública debe existir un plazo máximo de 6 meses.

Se debe implementar un mecanismo público y transparente que garantice la eliminación de las comunicaciones frente a los concesionarios y respecto a los datos que fueron transferidos a las autoridades.

La tercera *limitación* es otorgar facultades a un órgano supervisor, nos queda claro que la autoridad actúa discrecionalmente y que solo el 10% de las solicitudes de acceso a la retención de datos ha sido efectiva, lo cual significa que la actuación de las autoridades es violatoria de derechos humanos, por ello la existencia de un organismo supervisor, sancionador frente al abuso de las autoridades.

Una *cuarta limitación* para los concesionarios de telecomunicaciones es que deben implementar las medidas necesarias en seguridad, para asegurar la entrega solo a las autoridades competentes y garantizar que no serán transferidas total o parcialmente, a terceros. Asimismo, establecer perfiles las personas que podrán acceder y tratar los datos personales. De esta forma, sólo aquellos que cumplan con las características definidas podrán intervenir en el tratamiento de la conservación de las comunicaciones. Los casos en que la información deba ser entregada, transferidas se recomienda la encriptación con la finalidad de preservar la confidencialidad de los datos personales.

Necesitamos una cultura sobre la protección de los derechos y libertades propios de una democracia y por ello debemos continuar en la postura de establecer límites a las violaciones de derechos humanos en la protección de datos personales. La protección de datos está muy lejos de ser respetada por las autoridades por eso es necesario generar una estrategia para que las personas tengan conocimientos y exijan el uso correcto en las tecnologías de la información, donde los usuarios puedan exigir sus derechos ARCO y obligar a las autoridades que respeten los principios en el tratamiento y por otra parte exigir a los concesionarios que no realicen la retención de datos cuando se exceden en la finalidad de la prestación de un servicio.

BIBLIOGRAFIA Y CIBERGRAFÍA

Libros

ÁLVAREZ, Clara Luz, *Derechos de los usuarios de telecomunicaciones*, México, Instituto de Investigaciones Jurídicas UNAM, 2006.

ÁLVAREZ, Clara Luz, *Mexican Telecom Reform: Private Interest First",* México, Instituto de Investigaciones Jurídicas UNAM, Volumen 8, Número 1, México jul./dic. 2015.

ASOCIACIÓN MEXICANA DE DERECHO A LA INFORMACIÓN (AMEDI), *Panorama de la comunicación en México 2011: Desafíos para la calidad y diversidad,* México, Gráficos eFe, 2011

CARBONELL, MIGUEL, *El ABC de los derechos humanos y del control de convencionalidad*, México, Porrúa, 2015.

ESCALANTE LÓPEZ, Sonia, *Los derechos humanos en la seguridad pública y la función policial*, México, Editorial Flores, 2015

ESCUELA DE INTELIGENCIA Y SEGURIDAD NACIONAL (ESISEN), *Inteligencia y Seguridad Nacional*, México, ESISEN, 2009.

FERRER MAC-GREGOR, Eduardo y ZALDÍVAR LELO DE LARREA, Arturo (Coord), *La Ciencia del Derecho Procesal Constitucional,* Tomo IX, Derechos Humanos y Tribunales Internacionales*,* México, Instituto de Investigaciones Jurídica, UNAM, 2008.

FLORES PACHECO, Moisés Israel, "La geolocalización y el derecho a la privacidad. Análisis de la Acción de Inconstitucionalidad 32/2012*"*, *Estudios en Derecho a la*

Información, México, Instituto de Investigaciones Jurídicas UNAM, Número 1, ene/jun. 2016.

GARRIGA DOMÍNGUEZ, Ana, *Tratamiento de datos personales y derechos fundamentales*, Madrid España, Dykinson, 2009.

GÓMEZ-ROBLEDO VERDUZCO, Alonso y ORNELAS NÚÑEZ, Lina, *Protección de datos personales en México: el caso del Poder Ejecutivo, México*, Instituto de Investigaciones Jurídicas UNAM, 2006.

INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL DISTRITO FEDERAL (Infodf), *Retos de la protección de datos personales en el sector público,* México, Infodf, 2011.

JARDÓN PIÑA, Luis Manuel, *Criterios y jurisprudencia interamericana de derecho humanos: Influencia y repercusión en la justicia penal*, México, Instituto de Formación Profesional de la Procuraduría General de Justicia del Distrito Federal, 2014.

LUNA PLA, Issa (Coord), *Estudios aplicados sobre la libertad de expresión y el derecho a la información,* México, Instituto de Investigaciones Jurídica, UNAM, 2014.

LUNA PLA, Issa, et. al., *Resoluciones relevantes. En materia de acceso a la información y protección de datos personales*, México, Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, 2016.

COMISIÓN PARA EL ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS et. al, *Transparentemente: Protección de Datos Personales*, Privacidad en las Redes sociales, México, Comisión para el Acceso a la Información Pública y Protección de Datos (Puebla), 2012.

MIGUEL PÉREZ, Julio César, *Protección de datos y seguridad de la información*, Madrid, España, Ra-Ma, 2015.

MUÑOZ DÍAZ, Pablo Francisco, *Libertad de Expresión: Límites y Restricciones*, México, Escuela Libre de Derecho, 2016.

NAVARRO ISLA, Jorge (Coord), *Tecnologías de la Información y de las Comunicaciones: Aspectos Legales,* México, Porrúa, 2005.

NAVARRO SÁNCHEZ, Urenda Queletzú, *Seguridad Nacional: Reformas y Perspectivas*, México, Dirección Generak de Estudios Legislativos, Instituto Belisario Domínguez Senado de la República, 2011.

ORNELAS NUÑEZ, Lina Gabriela y ALCALDE URBINA, Samantha, *La protección de datos personales de menores en la era digital,* México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2014.

PAHUAMBA ROSAS, Baltazar (Coord), *Aplicación de los Derechos Humanos,* México, Novum, 2014, p. 140.

PESCHARD MARISCAL, Jacqueline, *Protección de Datos Personales. La voz de los actores,* México, Instituto Federal de Acceso a la Información Pública, 2010.

PONCE BAÉZ, Gabriela y GARCÍA TINAJERO, Leonel, *Las Fronteras del Derecho a la Información*, México, Novum, 2011.

REMOLINA ANGARITA, Nelson, *Tratamiento de datos personales: Aproximación Internacional y comentarios a la Ley 1581 de 2012,* Colombia, 2013.

SÁNCHEZ HERNÁNDEZ, Néstor Mauricio, *El derecho al acceso a la información y la protección de datos personales*, México, Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, 2016.

SOBERANES, José Luis, *Derechos humanos y su protección constitucional*, México, Porrúa, 2012.

VAZQUEZ, Daniel, *Test de razonabilidad y derechos humanos: Instrucciones para armar,* México, Instituto de Investigaciones Jurídicas UNAM, 2016.

VILLANUEVA, Ernesto, *Derecho de acceso a la información pública en Latinoamérica*, México, UNAM, 2003.

VILLANUEVA, Ernesto, *Régimen jurídico de las libertades de expresión e información en México*, México, Instituto de Investigaciones Jurídicas UNAM, 1998.

VILLANUEVA, Ernesto, *Seguridad nacional, información y poder legislativo*, disponible en https://archivos.juridicas. unam.mx/www/bjv/libros/5/2404/15.pdf

Revistas

ESCALANTE GONZALBO, Fernando, *"El Derecho a la privacidad"*, México, Instituto Federal de Acceso a la Información y Protección de Datos, Cuadernos de Transparencia, Número 2, 9ª reimpresión 2012.

MIRÓN REYES, Jorge Antonio, *Ataques a la vida privada y a la intimidad frente al derecho de acceso a la información*, Instituto de Investigaciones Jurídicas, disponible en: http://historico.juridicas.unam.mx/publica/rev/decoin/cont/8/art/art3.htm#N1

Cibergrafía

AOL, et. al., Reform Government Surveillance (*Reforma de la Vigilancia Gubernamental*), disponible en: https://www.reformgovernmentsurveillance.com/

CENTRO DE INVESTIGACIÓN Y SEGURIDAD NACIONAL (CISEN), disponible en http://www.cisen.gob.mx/snSegNal.html

CNDH. *Acción de Inconstitucionalidad 32/2010*, disponible en http://www.cndh.org.mx/sites/all/doc/Acciones/Acc_Inc_2012_32_Demanda.pdf

DIRECTIVA 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, disponible en http://ec.europa.eu/justice/data-protection/law/files/recast_20091219 _es.pdf

DIRECTIVA (UE) 2016/680 del Parlamento Europeo y del Consejo, *Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo*, http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES

DIRECTIVA 2006/24/CE del Parlamento Europeo y del Consejo del 15 de marzo de 2006, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*, disponible en: https://www.boe.es/doue/2006/105/L00054-00063.pdf

GACETA PARLAMENTARIA, año XVII, número 3916-V, jueves 28 de noviembre de 2013, *Proyecto de Decreto por el que se expide la Ley Federal de Telecomunicaciones y Radiodifusión, (Exposición de Motivos)*, disponible en http://gaceta.diputados.gob.mx/Gaceta/62/2013/nov/20131128-V.html#Iniciativa3

INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, 2015, disponible en: http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2015/

INSTITUTO NACIONAL DE TRANSPARENCIA ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI). *Posicionamiento de los Comisionados del IFAI, sobre la inconstitucionalidad de los artículos 30, 189 y 190, fracciones I, II y III de la Ley Federal de Telecomunicaciones y Radiodifusión.* Disponible en http://inicio.ifai.org.mx/nuevo/Posicionamientos%20de%20los%20Comisionados%20del%20IFAI.pdf

INSTITUTO NACIONAL DE TRANSPARENCIA ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, disponible en http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

RED EN DEFENSA DE LOS DERECHOS DIGITALES, *El Estado de la vigilancia fuera de control*, disponible en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016. pdf

RELATOR ESPECIAL DE LA NACIONES UNIDAS (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Libertad de Expresión y Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, *Declaración conjunta sobre programas de vigilancia*

y su impacto en la libertad de expresión, disponible en http://www.oas.org/es/cidh/expresion/ showarticle.asp?artID= 926&lID=2

RELATORÍA ESPECIAL PARA LA LIBERTAD DE EXPRESIÓN DE LA COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS DE LA OEA, *Libertad de Expresión e Internet*. Disponible en: http://www.oas.org/es/cidh/expresion /docs/informes/2014_04_08_internet_web.pdf

RELATORÍA ESPECIAL PARA LA LIBERTAD DE EXPRESIÓN COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, *Marco Jurídico Interamericano sobre el Derecho a la Libertad de Expresión*. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/MARCO%20JURIDICO%20INTERAMERICANO%20DEL%20DERECHO%20A%20LA%20LIBERTAD%20DE%20EXPRESION%20ESP%20FINAL%20portada.doc.pdf

SENTENCIA DEL TRIBUNAL DE JUSTICIA DE FECHA 8 DE ABRIL DE 2014. Directiva 2006/24/CE — Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones — Conservación de datos generados o tratados en relación con la prestación de tales servicios — Validez — Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea. Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&qid=148710 0101393&from=ES

Jurisprudencia

Tesis 2a./J. 69/2014 (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. I, junio de 2014, p. 555.

Tesis: Jurisprudencia (III Región) 5o. J/8 (10a.), *Gaceta del Semanario Judicial de la Federación,* Décima Época, t. II, 4 marzo de 2014, p. 1360

Tesis I.2o.A.E.34 A, *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. IV, agosto de 2016, p. 2528.

Tesis I.1o.A.E.73 A (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. IV, octubre de 2016, p. 4101.

Tesis 2a. XXXV/2016 (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. I, agosto de 2016, p. 776.

Tesis 2a. XLIV/2016 (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. II, agosto de 2016, p. 1305.

Tesis P./J. 130/2007, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXVI, diciembre de 2007, p. 8.

Tesis 1a. CCLXIII/2016 (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima Época, t. II, noviembre de 2016, p. 915.

Tesis 1a. CCLXX/2016 (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima Época, t. II, noviembre de 2016, p. 914.