Colección Ensayos para la Transparencia de la Ciudad de México 2013

22
Transparencia y gastos de campaña en las elecciones: dos eslabones para la legalidad y la legitimidad electoral en la ciudad de México.

Manuel Larrosa Haro

23
El derecho al olvido en relación con el derecho a la protección de datos personales.

Isabel Davara Fernández de Marcos

24
La protección de datos personales de menores en la era digital.

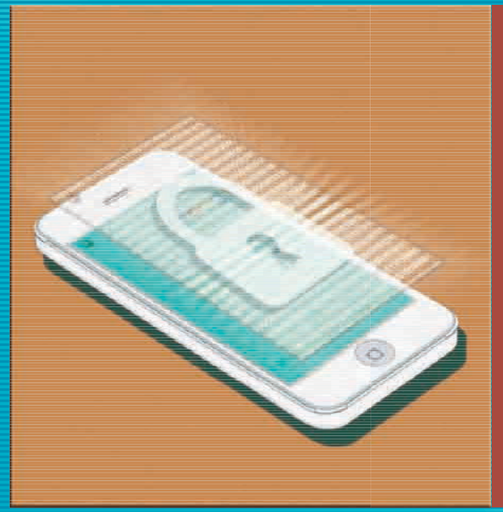
Lina Gabriela Ornelas Núñez y Samantha Alcalde Urbina

Invitamos a los lectores a consultar la página Web del Instituto, desde la cual tendrán acceso a todas nuestras publicaciones.

www.infodf.org.mx

infodf
Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal

La Morena No. 865 Local 1, Col. Narvarte Poniente,
Del. Benito Juárez, C.P. 03020, México, Distrito Federal
"Plaza de la Transparencia"
Tel. 5636-4636 (5636INFO) | www.infodf.org.mx | oip@infodf.org.mx



ensayos 25
PARA LA TRANSPARENCIA DE LA CIUDAD DE MÉXICO

La protección de datos en el ámbito de las telecomunicaciones e internet.

Miguel Recio Gayo

infodf
Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal

El Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF) pone a su disposición, la Colección de Ensayos para la Transparencia de la Ciudad de México, esfuerzo editorial dirigido a generar reflexión y análisis sobre el conocimiento y práctica de la transparencia, el acceso a la información, la protección de datos personales y la rendición de cuentas, en un contexto complejo como es el Distrito Federal, una de las ciudades más grandes del mundo.

Comprometido con la promoción de la cultura de la transparencia, el instituto, a través de su línea editorial Ensayos Científicos, impulsa el desarrollo de investigaciones acerca de estos componentes esenciales para el fortalecimiento de las democracias modernas, convocando a reconocidos investigadores y académicos a debatir y aportar ideas y experiencias, a través de este género que consideramos apropiado a los propósitos de divulgación del InfoDF.

Los ensayos pretenden ser puntos de partida para impulsar debates, documentar tendencias recientes, e incorporar análisis críticos y novedosos. Su estructura libre, su tratamiento sintético, la variedad temática, convierten al ensayo en un recurso pedagógico para inducir a todo público en el conocimiento y reflexión, que sin duda son necesarios para construir un pensamiento analítico en torno a estos nuevos conceptos que acompañan el fortalecimiento de las democrácias contemporáneas. Esperamos que los temas y el estilo personal de sus autores, inviten a la lectura y sobre todo, motiven su interés en participar en la discusión actual sobre estos temas y generar iniciativas que apoyen la consolidación de la cultura de transparencia en nuestra Ciudad de México.

25

LA PROTECCIÓN DE DATOS EN EL ÁMBITO DE LAS TELECOMUNICACIONES E INTERNET

MIGUEL RECIO GAYO

Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Primera edición, Diciembre 2015
ISBN: 978-607-95070-3-9
ISBN:

ÍNDICE

MIGUEL RECIO GAYO

Licenciado en Derecho por la Facultad de Derecho de la Universidad Carlos III de Madrid (España); maestro en Protección de Datos, Transparencia y Acceso a la Información por la Universidad CEU San Pablo (España); y maestro en Derecho de la Propiedad Intelectual por The George Washington University Law School (Estados Unidos).

Actualmente se desempeña como abogado experto en Derecho de las TIC en Madrid. Anteriormente trabajó como asesor legal para Latinoamérica en Business Software Alliance (BSA) en Washington, D.C., y en varias firmas jurídicas especializadas en Derecho de las TIC en Madrid.

Entre otras publicaciones, es autor de varias obras sobre protección de datos personales y firma electrónica tanto en México como en España.

INTRODUCCIÓN

Recuerda que cada transacción que haces,
cada sitio que visitas en Internet, deja huellas.[1]

Los servicios de telecomunicaciones,[2] y en particular Internet,[3] han dado lugar durante los últimos años, y lo siguen haciendo de manera constante, a importantes avances tecnológicos que facilitan las comunicaciones

[1] Traducción del original en inglés, *Remember that every transaction you make, every site you visit on the Internet leaves traces.* Recomendación núm. R(99)5 del Comité de Ministros del Consejo de Europa para la protección de la privacidad en Internet, adoptada por el Comité de Ministros el 23 de febrero de 1999.

[2] Por telecomunicaciones, conforme a la fracción LXVIII del artículo 3 de la Ley Federal de Telecomunicaciones y Radiodifusión (en adelante, LFTR), se entiende "toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión". Disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_140714.pdf>.

[3] La LFTR, ya citada, define Internet, en la fracción XXXII del artículo 3, como el "conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados intencionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única".

a distancia así como la posibilidad de acceder a innumerables servicios, como por ejemplo el correo electrónico, las redes sociales, la búsqueda de información, el comercio electrónico o la descarga de software o aplicaciones.

Desde el punto de vista del usuario, cuando éste es una persona física, ya sea mayor o menor de edad, es necesario ser consciente de que el uso de dichos servicios implica un tratamiento de sus datos personales.

Es así que, por ejemplo, cuando se llama por teléfono, se generan automáticamente registros relativos a la comunicación que incluyen, entre otros, el número de teléfono desde el que se llama, el número de teléfono al que se llama y cuánto tiempo ha durado la llamada. De igual forma, cuando se navega por Internet, puede generarse un rastro digital sobre, por ejemplo, qué página o sitio web se ha visitado y durante cuánto tiempo se ha estado conectado a la misma.

En estos casos, siempre que la información se refiera a una persona física[4] se produce un tratamiento de datos personales que queda sujeto tanto a la normatividad general como específica o sectorial aplicable en materia de protección de datos personales.

Además, el uso de dispositivos de telecomunicaciones u otros equipos tecnológicos plantea nuevas cuestiones, como por ejemplo la geolocalización en tiempo real,[5] o el "derecho al olvido" en relación con los motores de búsqueda o buscadores de Internet, sobre el que se ha pronunciado ya el Tribunal de Justicia de la Unión Europea (TJUE)[6] y que ha dado lugar a

[4] Es necesario recordar que las personas morales no están protegidas por el derecho fundamental a la protección de datos personales, de manera que se atiende al usuario que es persona física como titular de los datos personales objeto del tratamiento.

[5] Al respecto, puede verse la nota de prensa del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (en adelante, InfoDF) en la que el entonces comisionado ciudadano del InfoDF, Mucio Israel Hernández Guerrero, indicaba que "con la aprobación de la ley de telecomunicaciones se permite la geolocalización en tiempo real de las personas sin que medie una orden judicial, lo que es violatorio de los derechos humanos como el libre tránsito, el derecho a la privacidad, así como el debido proceso". Disponible en <http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=2005&Itemid=217>.

[6] Véase la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), del 13 de mayo de 2014, "Datos personales – Protección de las personas físicas en lo que respecta

un amplio debate tanto en la Unión Europea como en otros países, entre ellos México.[7]

Estos avances tecnológicos han centrado siempre la atención del legislador, de las autoridades de protección de datos y de otras autoridades competentes, ya que el uso más sencillo de los servicios de telecomunicaciones, por ejemplo, una llamada telefónica, tiene implicaciones tanto para el derecho fundamental a la protección de datos personales como para otros derechos protegidos constitucionalmente, tales como el secreto o la inviolabilidad de las comunicaciones.

Lo anterior implica que se deba prestar atención a la necesidad de proteger los derechos de los usuarios de telecomunicaciones e Internet para evitar vulneraciones del derecho a la protección de datos personales y la privacidad, como por ejemplo, evitar la retención indebida de datos personales relativos a telecomunicaciones, o el uso de los datos personales de los usuarios de telecomunicaciones con fines diferentes a la prestación del servicio cuando no se cumplen los requisitos de legitimación para el tratamiento, como por ejemplo, que dicho tratamiento esté previsto en una ley o se obtenga el consentimiento necesario del usuario.

Es por ello que el objeto del presente estudio es tratar cuestiones relativas a la necesidad de protección de datos personales en el ámbito

al tratamiento de dichos datos – Directiva 95/46/CE – Artículos 2, 4, 12 y 14 – Ámbito de aplicación material y territorial – Motores de búsqueda en Internet – Tratamiento de datos contenidos en sitios de Internet – Búsqueda, indexación y almacenamiento de estos datos – Responsabilidad del gestor del motor de búsqueda – Establecimiento en territorio de un Estado miembro – Alcance de las obligaciones de dicho gestor y de los derechos del interesado – Carta de los Derechos Fundamentales de la Unión Europea – Artículos 7 y 8", en el asunto C-131/12. Disponible en <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=208946>.

[7] Al respecto, cabe señalar que el comisionado presidente del InfoDF, Mucio Israel Hernández Guerrero, propuso su inclusión en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Véase la nota de prensa disponible en <http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=1522&Itemid=217>. También es una cuestión a la que se hizo referencia durante el XII Encuentro Iberoamericano de Protección de Datos, celebrado durante los días 12 y 13 de noviembre de 2014 en la Ciudad de México, tal y como consta en la nota de prensa disponible en <http://inicio.ifai.org.mx/Comunicados/Comunicado%20IFAI-129-14.pdf>.

de telecomunicaciones e Internet. Para tal fin, en primer lugar se presentan algunas cifras relevantes relativas al uso de las telecomunicaciones e Internet a nivel nacional y del Distrito Federal, de manera que sirvan para dimensionar el alcance de dichos servicios y el número de usuarios.

Tratar la protección de datos personales en el ámbito de las telecomunicaciones e Internet requiere prestar atención al derecho fundamental en sí mismo, distinguirlo de otros derechos fundamentales y presentar cuál es la normatividad general y la específica o sectorial en materia de protección de datos personales.

En la práctica, el uso de servicios de telecomunicaciones e Internet implica que se deban considerar, respectivamente, cuestiones específicas por lo que se refiere al tratamiento de datos personales. Es por ello que se dedican dos apartados específicos, uno relativo a las telecomunicaciones y otro a Internet, para las cuestiones más relevantes en materia de protección de datos personales.

A la vista del análisis hecho en los diferentes apartados, se presentan también las correspondientes conclusiones en materia de protección de datos personales en el ámbito de las telecomunicaciones e Internet.

Por último, se incluyen también algunas recomendaciones básicas dirigidas a las diferentes partes interesadas (el usuario, los proveedores y las autoridades garantes), con la finalidad de que puedan servirles, en cada caso, para la adopción de medidas que permitan fomentar el derecho fundamental a la protección de datos personales en particular en el ámbito de las telecomunicaciones e Internet.

1. EL USO DE LAS TELECOMUNICACIONES E INTERNET EN MÉXICO

A nivel nacional en México, los datos del Instituto Federal de Telecomunicaciones (IFT) disponibles en 2014, mostraban que el número de suscripciones de telefonía móvil y fija ascendían con respecto a años anteriores. Y también a nivel nacional, según los datos del Instituto Nacional de Estadística y Geografía (INEGI), el número de usuarios de Internet durante el primer trimestre de 2014 había aumentado con respecto a los años previos.

En el caso del Distrito Federal, por lo que se refiere al uso de Internet, según los datos disponibles y referidos a 2014, los principales usos eran para obtener información (77.5%), para comunicarse (51.2%), para acceder a redes sociales (34.9%), para apoyar la educación/capacitación (33.2%), para entretenimiento (31.4%) y para otros fines, tales como interactuar con el gobierno. Por lo que se refiere al dispositivo más utilizado para acceder a Internet, la computadora de escritorio era, en 2014, el más utilizado, seguido por la computadora portátil o laptop, el teléfono celular y otros dispositivos.

Y conforme a las cifras del INEGI, publicadas en abril de 2014, más del 10% de los usuarios de Internet en México son del Distrito Federal (resumen del capítulo elaborado por el autor del ensayo).

Antes de analizar las diversas cuestiones que se plantean en relación con el tratamiento de datos personales en las telecomunicaciones e Internet, cabe hacer una referencia general al uso de estos servicios en México. De esta manera, será posible dimensionar el alcance y significado del derecho fundamental a la protección de datos personales en este ámbito.

Según los datos del Instituto Federal de Telecomunicaciones (IFT)[8] del tercer trimestre de 2014, en

[8] Sobre el IFT puede verse más información en el vínculo electrónico <http://www.ift.org.mx>.

cuanto a la telefonía móvil y fija a nivel nacional, cabe destacar lo siguiente:[9]

- **Número de suscripciones de telefonía móvil.** El total era de 102.2 millones, lo que supone que el número de suscripciones sea de 85.4 por cada 100 habitantes. Del número total de suscripciones de telefonía móvil, por modalidad de contratación, 15.3 millones son de pospago (15% del total de suscripciones) y 86.8 millones de prepago (85% del total de suscripciones). En cuanto a la banda de ancha móvil, al tercer trimestre de 2014, la penetración era de 44.3 suscriptores por cada 100 habitantes.

- **Número de suscripciones de telefonía fija.** El número total de suscripciones de telefonía fija, al cierre del tercer trimestre de 2014, era 20.64 millones, lo que suponía una densidad de 17.2 suscripciones de telefonía fija por cada 100 habitantes.

Por lo que se refiere al uso de Internet, según el *Estudio sobre los hábitos de los usuarios de Internet en México 2015*,[10] de la Asociación Mexicana de Internet (AMIPCI),[11] el número de usuarios de Internet en México en el año 2014 era de 53.9 millones, lo que supone 5.3% más con respecto a 2013, cuando el total de usuarios alcanzó los 51.2 millones.[12]

[9] Al respecto, véase el *Informe estadístico 3er trimestre de 2014*. Disponible en http://www.ift.org.mx/sites/default/files/contenidogeneral/comunicacion-y-<medios/informe3ertrimestre2014.pdf>.

[10] Este estudio, presentado durante el Día de Internet 2015, está disponible en el vínculo electrónico <https://www.amipci.org.mx/images/AMIPCI_HABITOS_DEL_INTERNAUTA_MEXICANO_2015.pdf>.

[11] El nombre original de la AMIPCI era el de Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, A.C. Al respecto, puede verse lo indicado en <https://www.amipci.org.mx/es/que-es>.

[12] Conforme a lo indicado por la AMIPCI en su estudio, los datos sobre usuarios de Internet se basan en las cifras en millones calculadas con base en información del INEGI e IFETEL. Véase el estudio ya citado.

Por su parte, según los datos del Instituto Nacional de Estadística y Geografía (INEGI)[13] en cuanto al número de usuarios de Internet,[14] considerando como tales a personas con seis años o más de edad usan Internet por sí mismos, cabe señalar que, a finales de 2013, el número total era de 46 026 450 usuarios y, en abril de 2014, la cifra de usuarios de Internet había ascendido a 47 441 244 usuarios.[15]

En cuanto a los principales usos de Internet, también según las cifras preliminares de INEGI en el mes de abril de 2014 eran los siguientes:[16]

Nacional		
Tipo de uso	Número total de usuarios	Por ciento
Usuarios de Internet	**47 441 244**	**100**
Obtener información	31 972 711	67.4
Comunicarse	18 265 615	38.5
Entretenimiento	17 198 224	36.3
Apoyar la educación/capacitación	17 393 808	36.7
Acceder a redes sociales	18 796 019	39.6
Operaciones bancarias en línea	693 955	1.5
Interactuar con el gobierno	594 580	1.3
Otros usos	434 860	0.9
No especificado	24 646	0.1

[13] Sobre el INEGI puede verse más información en <http://www.inegi.org.mx>.

[14] Siendo definido el usuario de Internet por el INEGI como: "Individuo de seis o más años que en forma eventual o cotidiana, y de manera autónoma, ha accedido y realizado alguna actividad en Internet en los últimos seis meses. Las actividades pueden ser, entre otras, para realizar tareas escolares; las relacionadas con el trabajo; de comunicación, incluyendo correos electrónicos o conversaciones escritas (chat); de capacitación, adiestramiento o formación a distancia mediante videoconferencias; de entretenimiento, como son las de bajar o jugar videojuegos o programas de computadora en la red, como son los de música." Disponible en <http://www3.inegi.org.mx/sistemas/sisept/glosario/default.aspx?t=tinf204&e=00&i=>.

[15] Véase la información y téngase en consideración las notas aclaratorias. Disponible en <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tinf204&s=est&c=19437>.

[16] Disponible en <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tinf229&s=est&c=26482>.

Y referidos específicamente al Distrito Federal, los datos relativos a los principales usos de Internet, conforme al INEGI,[17] son los siguientes:

Distrito Federal		
Tipo de uso	Número total de usuarios	Por ciento
Usuarios de Internet	**5 019 415**	**100**
Obtener información	3 889 609	77.5
Comunicarse	2 570 723	51.2
Entretenimiento	1 575 390	31.4
Apoyar la educación/capacitación	1 664 131	33.2
Acceder a redes sociales	1 750 181	34.9
Operaciones bancarias en línea	123 922	2.5
Interactuar con el gobierno	100 522	2
Otros usos	190 182	3
No especificado	1 462	0

A la vista de estas cifras, cabe señalar que más de 10% de los usuarios de Internet en México son del Distrito Federal. Se trata de una cifra relevante ya que se trata de un tanto por cien sustancial en comparación con el número total de usuarios de Internet a nivel nacional.

En cuanto a los dispositivos utilizados a nivel nacional para acceder a Internet, en 2014, conforme a las cifras preliminares al mes de abril según los datos del INEGI,[18] el equipo o dispositivo más utilizado fue la computadora de escritorio (34 851 977 usuarios), seguida por la computadora portátil o laptop (16 436 052 usuarios) y el teléfono celular, iPhone o similar (9 415 431 usuarios). Otros dispositivos serían los equipos de bolsillo sin función telefónica (PocketPC, PDA).

[17] Disponible en <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tinf255&s=est&c=28978>.

[18] Disponible en <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tinf231&s=est&c=26484>.

Por último, con respecto a las cifras a nivel nacional sobre el uso de Internet por género, conforme a los datos del INEGI,[19] el total de 47 441 244 se divide casi al 50%, ya que 23 762 805 usuarios son hombres (50.1%) y 23 678 439 usuarios son mujeres (49.9%).

Cabe destacar que contar con cifras como éstas permite, en su caso, saber qué tipo de usuarios de servicios de telecomunicaciones e Internet hay tanto a nivel nacional como del Distrito Federal o de los estados; también el uso de dispositivos o equipos y, por lo tanto, servir de base para, en su caso, promover o adoptar medidas que tengan por objeto fomentar la protección de los datos personales y la privacidad. Además, estas cifras pueden servir también de base en el análisis de cuestiones interrelacionadas con el derecho a la protección de datos personales, tales como la protección de los consumidores o el derecho de la competencia.

[19] Disponible en <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tinf216&s=est&c=19445>.

2. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y OTROS DERECHOS FUNDAMENTALES

La Constitución Política de los Estados Unidos Mexicanos reconoce los derechos fundamentales a la protección de datos personales y a la inviolabilidad o secreto de las comunicaciones. Se trata de dos importantes derechos que protegen a la persona en cuanto al uso que hace o puede hacer de los servicios de telecomunicaciones, ya sean servicios de telefonía o Internet.

Además, hay otros derechos que también están reconocidos en la Constitución, como el acceso a las tecnologías de la información y comunicación, incluyendo la banda ancha e Internet. En particular, estos derechos son consecuencia de las reformas constitucionales llevadas a cabo en 2014 y que dieron también lugar a la publicación de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) que, entre otras cuestiones, establece los derechos de los usuarios de servicios de telecomunicaciones e Internet, entre los que se encuentran tanto el derecho de acceso a dichas tecnologías como el derecho de privacidad.

Por lo que se refiere a la protección de datos personales, este derecho fundamental en el ámbito de las telecomunicaciones e Internet, proporcionados por sujetos obligados en México, está protegido tanto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento, que constituyen la normatividad general, como por la Ley Federal de Telecomunicaciones y Radiodifusión, así como por otra normatividad específica aplicable en el sector de las telecomunicaciones y a la protección de los consumidores (resumen del capítulo elaborado por el autor del ensayo).

2.1. Previsiones en la Constitución

La Constitución Política de los Estados Unidos Mexicanos (en adelante, CPEUM) reconoce tanto el derecho a la protección de datos personales como el derecho al secreto o inviolabilidad de las comunicaciones.

En el caso de la protección de datos personales, este derecho se encuentra previsto, para el sector privado, en el segundo párrafo del artículo 16 constitucional,[20] que indica: "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." Y como veremos a continuación, la ley que desarrolla lo previsto en dicho artículo es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.[21]

El hecho de que la protección de datos personales en el sector privado haya sido regulada por una ley federal, se debe a que la competencia se atribuye al Congreso Federal en virtud de la reforma al artículo 73 constitucional[22] que se llevó a cabo en 2009. En concreto, se adicionó la fracción XXIX-O al citado artículo para atribuirle la competencia para legislar en la materia.

La razón para conferir al Congreso Federal la competencia en materia de protección de datos personales se debe a que, de otro modo, podrían crearse paraísos de datos personales, interponer obstáculos o barreras al comercio al interior de la República, además de garantizar así un mismo nivel de protección a los titulares de este derecho. Es decir, se trata de garantizar también el libre flujo de los datos personales, evitando barreras al comercio y a la necesidad de garantizar, de manera uniforme, el derecho fundamental a la protección de datos personales.

[20] La redacción de este párrafo segundo del artículo 16 constitucional se debe a la reforma producida en virtud del decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el *Diario Oficial de la Federación* el 1 de junio de 2009. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf>. El texto de la Constitución, con las sucesivas reformas hechas hasta el 9 de julio de 2015, está disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/1_020715.pdf>.

[21] Publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.

[22] Véase el Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el *Diario Oficial de la Federación* el 30 de abril de 2009. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_185_30abr09.pdf>.

El derecho a la protección de datos personales[23] se concreta, para el titular de los datos personales, en "el poder de decidir y controlar si un tercero puede transmitir o utilizar sus datos que van desde el teléfono o domicilio, hasta su religión".[24] Es decir, es el poder de control de la persona física, titular de los datos, sobre quién, cómo y para qué se usan sus datos personales.

La privacidad es un concepto más amplio que el de la protección de datos personales, si bien ambos coinciden en el control sobre los datos personales por su titular.[25]

---

[23] Sobre el significado y alcance de este derecho, puede verse el capítulo de Jacqueline Peschard Mariscal, "El derecho fundamental a la protección de datos personales en México", *La protección de datos personales en México*, México, Tirant lo Blanch, 2013, pp. 19-38.

[24] Véase el Dictamen de la Comisión de Gobernación con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, p. 25. Disponible en <http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf>.

[25] Al respecto, véase José Luis Piñar Mañas (2010), "¿Existe privacidad?", *Protección de datos personales. Compendio de lecturas y legislación*, México, Tiro Corto Editores. El autor indica que "no es nada sencillo definir la privacidad" (p. 16). Y a continuación se refiere también al concepto de privacidad manejado por Warren y Brandeis, así como a que él mismo "ha sido desde luego superado", y menciona también a Westin, quien "identificó cuatro tipos de privacidad, que PEDERSEN amplió hasta cinco: soledad, aislamiento, reserva, intimidad y anonimato" (p. 14). Por su parte, Daniel Solove, mencionado en el estudio del Parlamento Europeo titulado *Does it help or hinder? Promotion of Innovation on the Internet and Citizens´ Right to Privacy*, identifica hasta seis aproximaciones a la privacidad: "1) The right to be let alone; 2) Limited access to the self-recognition of concealment and limited access to others; 3) Secrecy; 4) Control over personal information; 5) Personhood; 6) Intimacy" (p. 23). También sobre el concepto de privacidad puede verse a Arthur R. Miller (1971), *The Assault on Privacy: Computers, Data Banks, and Dossiers*, Michigan, University of Michigan Press. En concreto, el autor indica que "The concept of privacy is difficult to define because it is exasperatingly vague and evanescent, often meaning strikingly different things to different people. In part this is because privacy is a notion that is emotional in its appeal and embraces a multitude of different 'rights', some of which are intertwined, others often seemingly unrelated or inconsistent" (p. 25). Lo que puede traducirse al español como "El concepto de privacidad es difícil de definir porque es exasperantemente vago y evanescente, a menudo significa sorprendentemente cosas diferentes para diferentes personas. En parte, esto se debe a que la privacidad es una noción que es emocional en su apelación y abarca una multitud de diferentes 'derechos', algunos de los cuales están entrelazados, otros a menudo sin aparente o inconsciente relación."

El Dictamen de la Comisión de Gobernación con Proyecto de Decreto por el que se expide la LFPDPPP, indica: "los orígenes del derecho a la protección de los datos personales, en cuanto a derecho autónomo respecto de la privacidad y la intimidad, se ubican en Europa",[26] y en este sentido es posible afirmar que la privacidad se corresponde con el derecho fundamental a la vida privada consagrado en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea,[27] y que encuentra su referente en el artículo 8, relativo al respeto a la vida privada y familiar, del Convenio Europeo de Derechos Humanos.[28]

Por su parte, el derecho fundamental a la protección de datos personales es un derecho autónomo, independiente del derecho fundamental a la vida privada. Siguiendo con la referencia a la Carta de los Derechos Fundamentales de la Unión Europea, el artículo 8 es el que incluye el derecho a la protección de datos personales.[29]

---

[26] Véase José Luis Piñar Mañas, *op. cit*., p. 17.

[27] En Europa, este derecho fundamental a la vida privada está consagrado en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea, que lo enuncia así:
Artículo 7
Respeto a la vida privada y familiar
Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
La Carta de los Derechos Fundamentales de la Unión Europea fue publicada en el *Diario Oficial de la Unión Europea*, núm. C 364, del 18 de diciembre de 2000. Disponible en <http://www.europarl.europa.eu/charter/pdf/text_es.pdf>.

[28] El artículo 8 del citado Convenio indica lo siguiente:
Artículo 8
Derecho al respeto a la vida privada y familiar
1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.
El Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convenio Europeo de Derechos Humanos) fue abierto para su firma en Roma el 4 de noviembre de 1950, y entró en vigor, tras lograrse 10 ratificaciones, el 3 de septiembre de 1953. El texto puede verse, en una traducción no oficial al español, en <http://www.echr.coe.int/Documents/Convention_SPA.pdf>.

[29] El citado artículo indica:
Artículo 8
Protección de datos de carácter personal

Privacidad, o vida privada, y protección de datos personales son, por lo tanto, derechos fundamentales independientes, con contenido propio, de manera que el derecho fundamental a la protección de datos personales, ya estén éstos en posesión de sujetos de carácter público o privado, se refiere a un aspecto muy específico: el control sobre el tratamiento (legítimo, controlado e informado) de los datos personales por su titular, pero que también es clave para garantizar la privacidad y otros derechos fundamentales.

Por lo que se refiere a otros derechos fundamentales, una de las principales razones de la reforma en materia de telecomunicaciones era ampliarlos, en particular con respecto a la privacidad y al acceso a las tecnologías de la información y comunicación, así como a los servicios de telecomunicaciones, banda ancha e Internet.

En materia de privacidad, hay que poner también atención al derecho al secreto o inviolabilidad de las comunicaciones, contemplado en el decimosegundo párrafo del artículo 16 constitucional, que indica que "las comunicaciones privadas son inviolables".[30]

La Suprema Corte de Justicia de la Nación (SCJN) tuvo oportunidad de pronunciarse sobre la inviolabilidad de las comunicaciones privadas, al resolver el amparo en revisión 2/2000, mediante sesión pública de la Segunda Sala celebrada el día 11 de octubre de 2000, donde analizó la intervención de las conversaciones telefónicas, las circunstancias en las

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

30 Y el párrafo siguiente indica que: "Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor."

que conforme a la ley una intervención de las comunicaciones privadas es lícita, así como el derecho a la privacidad como garantía individual.

Como se expone en la crónica[31] elaborada por la SCJN sobre dicho amparo en revisión, la reforma constitucional en los párrafos noveno y décimo del artículo 16,

> […] tuvo la finalidad de otorgar un fundamento a la adopción de nuevas estrategias que permitieran la investigación del crimen organizado por parte de los órganos policiacos, y dentro de dichas estrategias se encontraba la intervención de medios privados de comunicación; no obstante, se tomaron medidas para evitar la vulneración de las garantías constitucionales como lo es el derecho a la intimidad o a la vida privada, por lo que se condicionó dicha intervención a la autorización de una autoridad judicial federal, previa solicitud de autoridad competente que cumpla con la fundamentación, motivación y especificación de ciertos requisitos, además de que previó la prohibición de las autorizaciones correspondientes en determinadas materias y circunstancias, tal como en la materia civil.[32]

La crónica refleja también que la respuesta de la sociedad fue de cautela y de duda sobre la constitucionalidad de dicha medida. Y, sin perjuicio de lo anterior, los requisitos necesarios y límites previstos en la Constitución son los criterios que han de seguirse en todo momento y caso para determinar si una intervención de las comunicaciones es lícita o no.

Es así que las comunicaciones privadas, ya sean postales, telefónicas o electrónicas, son inviolables, como se prevé en el artículo 16, párrafo noveno constitucional. Esto significa que

> […] corresponde a la autoridad judicial federal, a petición de la autoridad federal facultada por la ley o del titular del Ministerio

[31] Véase Suprema Corte de Justicia de la Nación (2006), "Inviolabilidad de las comunicaciones privadas", *Serie de crónicas de asuntos relevantes del Pleno y las Salas de la Suprema Corte de Justicia de la Nación*. Disponible en <https://www.scjn.gob.mx/Cronicas/Cronicas%20del%20pleno%20y%20salas/cr_inv_comunic.pdf>.

[32] *Ibidem*, p. 8.

> Público de la entidad federativa que corresponda, autorizar la intervención de cualquier comunicación privada, siempre que la petición se haga por escrito, y en ésta se funden y motiven las causas legales de la solicitud, se indique el tipo de intervención, los sujetos de la misma y su duración.[33]

Así pues, se trata de un derecho fundamental que, al igual que la protección de datos personales, vincula tanto a las autoridades públicas como a los sujetos privados. Y en este caso lo que se protege es el contenido de la comunicación, con independencia del medio por el que se produzca, lo que a su vez puede implicar también un tratamiento de datos personales que debe cumplir con las correspondientes garantías constitucionales, normativas y regulatorias.

Incidiendo de nuevo en la explicación sobre la reforma de las telecomunicaciones, cabe señalar que "se establece con claridad que la información transmitida a través de las redes y servicios de telecomunicaciones será confidencial, salvo aquella que por su propia naturaleza sea pública, o cuando medie orden de autoridad judicial competente".[34]

En ese sentido, como garantía, la LFTR incluye como infracción sancionable con multa[35] la acción consistente en "interceptar información que se transmita por las redes públicas de telecomunicaciones, salvo que medie resolución de autoridad competente" (fracción III del apartado D del artículo 298). El uso del término "autoridad competente" suscita muchas dudas razonables, máxime si esta previsión se considera a la vista del artículo 16 de la Constitución. Urge, por lo tanto, que dichas dudas sean despejadas para evitar riesgos potenciales de intromisiones indebidas en los derechos fundamentales, de manera que, quien sean competente, ya sea el legislador, el juez, la autoridad garante o reguladora u otra, o todas a la vez, actúen de manera decidida y sin dilación.

[33] *Ibidem*, p. 11.

[34] Véase el documento del Gobierno de la República titulado *Reforma en materia de telecomunicaciones*, p. 17. Disponible en <http://reformas.gob.mx/wp-content/uploads/2014/06/EXPLICACION_AMPLIADA_DE_LA_REFORMA_EN_MATERIA_DE_TELECOMUNICACIONES.pdf>.

[35] En concreto, multa "por el equivalente del 2.01% hasta 6% de los ingresos del concesionario o autorizado".

Sin perjuicio de esta obligada referencia al derecho al secreto o inviolabilidad de las comunicaciones privadas, atenderemos a continuación de manera concreta al derecho a la protección de datos personales, tanto en las telecomunicaciones como en Internet.

Otro derecho fundamental previsto en la Constitución, como consecuencia de las reformas llevadas a cabo,[36] es el derecho de acceso a las tecnologías de la información y la comunicación, lo que incluye tanto la banda ancha como el Internet.

En concreto, el tercer párrafo del artículo 6 constitucional[37] indica que "el Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet."

Al ser considerados los servicios de telecomunicaciones como servicios públicos de interés general[38] "el Estado garantizará que sean prestados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin injerencias arbitrarias", tal y como indica el artícul o 6 de la CPEUM, apartado B, fracción II, lo que implica que todas las personas deban tenerlo garantizado.

En este sentido, el gobierno de la República puso en marcha el proyecto México Conectado con la finalidad de garantizar el derecho constitucional de acceso a Internet a través de sitios y espacios públicos tales como escuelas, centros comunitarios o parques a nivel federal, estatal y municipal.[39]

---

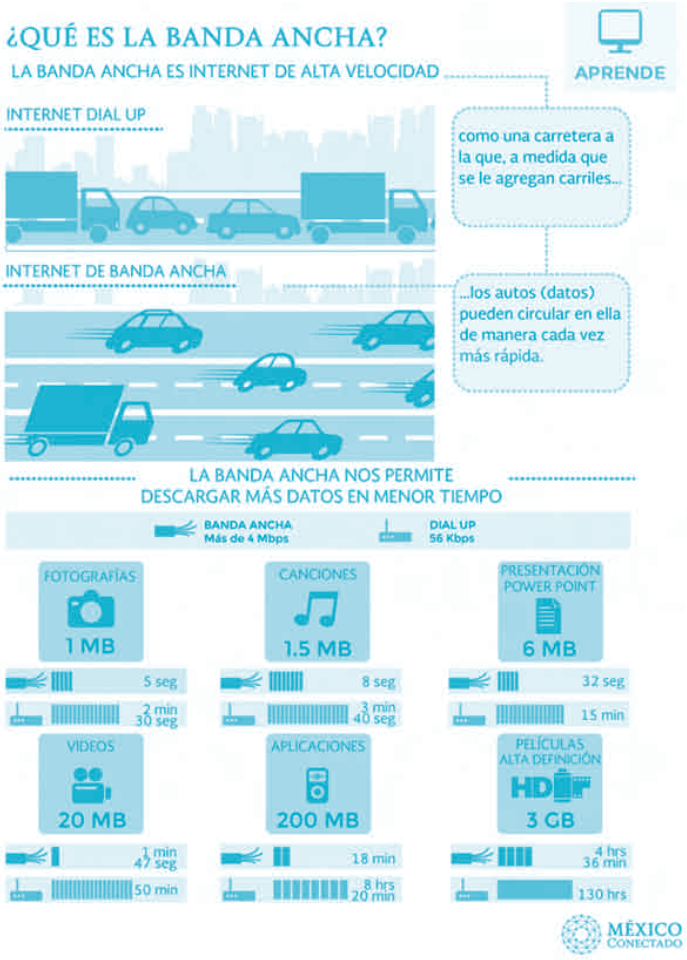
[36] Estas reformas en telecomunicaciones y en otros ámbitos como el energético o el laboral, eran parte de un paquete de reformas estructurales que fue el resultado de un diagnóstico llevado a cabo por el gobierno federal para la construcción de un nuevo México.

[37] Es un párrafo adicionado en virtud del Decreto publicado en el *Diario Oficial de la Federación* el 11 de junio de 2013.

[38] En relación con el concepto de servicio público, puede verse a Mauricio Yanome Yesaki, *El concepto de servicio público y su régimen jurídico en México*, Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM. Disponible en <http://biblio.juridicas.unam.mx/libros/6/2544/31.pdf>.

[39] Sobre el proyecto México Conectado, puede verse más información en <http://mexicoconectado.gob.mx/index.php/sobre-mexico-conectado>. También, los

Este acceso, en sitios públicos, se llevará a cabo a través de la banda ancha, que permite hacer uso de Internet de alta velocidad, lo cual es importante para acceder de manera adecuada a servicios o contenidos electrónicos. A continuación se incluye una breve explicación sobre qué significa la banda ancha, según la información disponible en el sitio web del proyecto México Conectado:



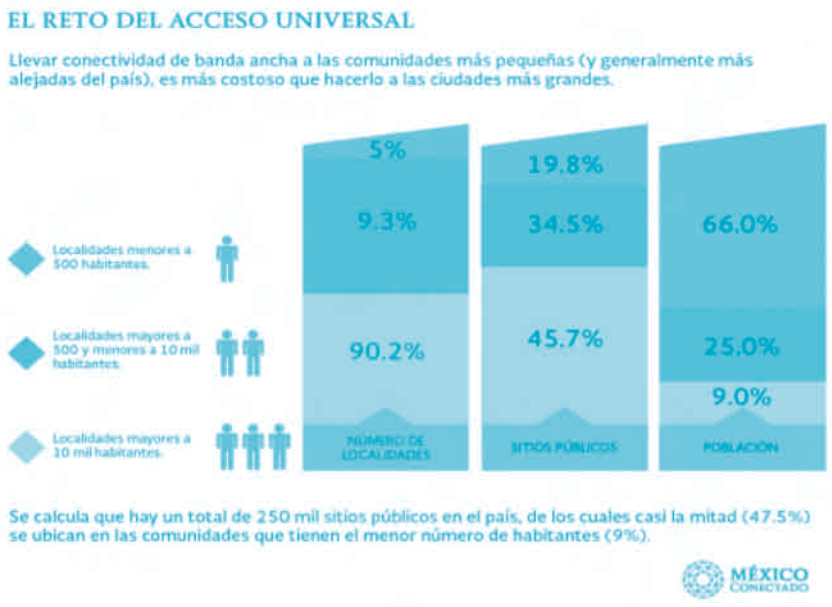
Fuente: <http://mexicoconectado.gob.mx/index.php/component/k2/item/179-que-es-banda-ancha?Itemid=145>.

Lineamientos del Proyecto México Conectado, disponibles en <http://mexicoconectado.gob.mx/images/archivos/Lineamientos_Mexico_Conectado.pdf>.

Cabe señalar que el proyecto México Conectado tiene como objetivo conseguir proveer conectividad de banda ancha a más de 250 000 sitios de acceso público para 2018. Este objetivo pasa por considerar que, según las cifras ofrecidas por el proyecto México Conectado, estos 250 000 sitios y espacios públicos están dispersados geográficamente por todo el país, incluso en localidades con poblaciones pequeñas (de menos de 500 habitantes) que todavía no cuentan con los medios necesarios para acceder a una conexión a Internet. En cuanto a la distribución de los sitios y espacios públicos y de la población a los que se quiere dar la posibilidad de que puedan tener una conexión de banda ancha a Internet, México Conectado calcula que en localidades de menos de 500 habitantes, lo que supone 9% del total de la población y representa 90.2% del total de las localidades del país, hay 47.5% de los 250 000 sitios públicos. En el caso de las localidades con más de 500 habitantes y menos de 10 000, lo que supone 25% del total de la población y representa 9.3% de las localidades del país, el número de sitios públicos es 34.5% de los 250 000 sitios públicos. Por último, las localidades con más de 10 000 habitantes, donde se concentra 66% de la población y que supone 0.5% del total de localidades del país, el número de sitios públicos es 19.8% del total.

El reto del acceso universal[40] se resume gráficamente de la siguiente manera:

[40] Por lo que se refiere a la meta del proyecto México Conectado, puede verse la nota de prensa de la Secretaría de Comunicaciones y Transportes (SCT) disponible en <http://mexicoconectado.gob.mx/index.php?option=com_k2&view=item&Itemid=143&id=5:mas-de-45-mil-puntos-publicos-de-acceso-a-la-banda-ancha-en-mexico>.



Fuente: <http://mexicoconectado.gob.mx/sobre_mexico_conectado.php?id=69>.

2.2. Normatividad general sobre protección de datos personales

En materia de protección de datos personales, en el sector privado, la normatividad general aplicable a nivel federal a los servicios de telecomunicaciones e Internet proporcionados por concesionarios de telecomunicaciones, autorizados o proveedores establecidos en México o sujetos a la misma, es la ya citada LFPDPPP y su Reglamento.[41]

[41] Se trata del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *Diario Oficial de la Federación* del 21 de diciembre de 2011. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf>.

La LFPDPPP se ve complementada por diversas disposiciones que se refieren, en particular, al aviso de privacidad[42] y a los Parámetros de autorregulación en materia de Protección de Datos Personales.[43]

Que se haga referencia a esta normatividad como general en materia de protección de datos personales debe ser entendido en el sentido de que puede haber normatividad sectorial específica, tal y como ocurre con la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR).

Los sujetos obligados que tienen que cumplir con dicha normatividad son los particulares, ya sean personas físicas o morales, como por ejemplo los concesionarios que proporcionan servicios de telecomunicaciones, o el editor de una página o sitio web establecidos en México sujetos a la normatividad mexicana en la materia.

Si dichas personas deciden sobre el tratamiento de los datos personales del usuario de los correspondientes servicios, por ejemplo para prestarle el servicio de telefonía o para enviarle publicidad de sus servicios, entonces serán consideradas como responsables del tratamiento.[44] En otro caso, si tratan los datos personales por cuenta de terceros que deciden sobre el tratamiento de los datos personales, serían considerados como encargados del tratamiento.

[42] En cuanto al aviso de privacidad, véanse los "Lineamientos del Aviso de Privacidad", publicados en el *Diario Oficial de la Federación* del 17 de enero de 2013. Disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013>. Al respecto, tómense también en cuenta los "Criterios generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos", publicados en el *Diario Oficial de la Federación* del 18 de abril de 2012 y disponibles en <http://www.dof.gob.mx/nota_detalle.php?codigo=5244229&fecha=18/04/2012>. Por último, en relación con estos criterios generales, puede verse la *Guía del INAI* para instrumentar medidas compensatorias, publicada en mayo de 2014 y disponible en <http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_para_instrumentar_medidas_compensatorias.pdf>.

[43] Véase *Diario Oficial de la Federación*, 29 de mayo de 2014. Disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014>. Estos parámetros, en virtud de su artículo transitorio segundo, abrogan los parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *DOF* el 17 de enero de 2013, así como su modificación, publicada en el *DOF* el 16 de julio de 2013.

[44] Figura a la que se define en la fracción XIV del artículo 3 de la LFPDPPP como "Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales."

En concreto, el responsable del tratamiento tiene que manejar los datos personales de los titulares de los datos con apego a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Los principios, conforme a lo previsto en la LFPDPPP y su Reglamento, pueden resumirse esquemáticamente de la siguiente manera:

Principio	Desarrollo			
Lealtad	Expectativa razonable de privacidad			
	Prohibición de obtener datos personales por medios engañosos o fraudulentos			
Consentimiento	Forma	Tácito		
		Expreso	— Verbal — Escrito	
	Características de la manifestación de voluntad	— Libre — Específica — Informada — Inequívoca		
	Regla general	Necesidad del consentimiento (tácito o expreso, según el supuesto)		
	Excepciones	— Al tratamiento — A la transferencia (nacional o internacional)		
	Revocación			
	Prueba			
Información	Aviso de privacidad	Documento	— Físico — Electrónico — En cualquier otro formato	
		Características	— Sencillo — Expresado con lenguaje claro y comprensible — Con una estructura y diseño que facilite su entendimiento — Con información necesaria	
		Contenido		
		Puesta a disposición	— Previo al tratamiento	
		Formatos	— Físicos — Electrónicos — Medios electrónicos — Cualquier otra tecnología	
	Obtención de los datos personales			
	Medidas compensatorias			
	Prueba			
Calidad	Los datos personales serán	— Exactos — Completos — Pertinentes — Correctos — Actualizados	Para los fines para los cuales fueron recabados	
	Adoptar medidas razonables de acuerdo con		— Tipo de datos personales — Condiciones del tratamiento	
Finalidad	Cumplimiento de la(s) finalidad(es) prevista(s) en el aviso de privacidad	— Con claridad — Sin lugar a confusión — De manera objetiva se especifica para qué objeto serán tratados los datos personales		
	Finalidades	— Primarias: dieron origen y son necesarias para la relación jurídica entre el responsable y el titular — Secundarias		
		— No se pueden tratar para finalidades distintas que no sean compatibles o análogas con aquellas para los que se hubiesen recabado	A menos que: — Lo permita de forma explícita una ley o reglamento — El responsable haya obtenido el consentimiento para el nuevo tratamiento	
Lealtad	Sólo podrán crearse bases de datos que contengan datos personales sensibles cuando	— Obedezca a un mandato legal — Se justifique por motivos de límites previstos en la ley — El responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga		
Proporcionalidad	Datos personales	— Pertinentes — Necesarios — Adecuados — Relevantes	Finalidades para las que hayan sido obtenidos	
	Minimización	Limitar al mínimo el tratamiento de acuerdo con la finalidad		
Responsabilidad	Velar y responder por el tratamiento de los datos personales que	— Estén bajo su custodia o posesión — Sean tratados por un encargado		

Fuente: Miguel Recio Gayo (2013), *Esquemas de la Ley de Protección de Datos Personales y su Reglamento*, México, Tirant lo Blanch, pp. 29-42.

Y dicho tratamiento de datos personales tendrá que hacerse también observando los deberes de seguridad y confidencialidad. De manera resumida y esquemática, estos deberes pueden presentarse de la siguiente manera:

Deber	Desarrollo		
Medidas de seguridad	Responsable y encargado del tratamiento		
	Control o grupo de controles de seguridad para proteger los datos personales		— Administrativas — Técnicas — Físicas
	Proteger los datos personales contra		— Daño — Pérdida — Alteración — Destrucción
			No autorizado
			— Uso — Tratamiento — Acceso
	Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información		
	Factores para determinar las medidas de seguridad		— El riesgo inherente por tipo de dato personal — La sensibilidad de los datos personales tratados — El desarrollo tecnológico — Las posibles consecuencias de una vulneración para los titulares — El número de titulares — Las vulnerabilidades previas ocurridas en los sistemas de tratamiento — El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión — Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable
	Acciones para la seguridad de los datos personales		
	Eventos en los que se deberán actualizar las medidas de seguridad		
Vulneraciones de seguridad	Ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares		— La pérdida o destrucción no autorizada — El robo, extravío o copia no autorizada — El uso, acceso o tratamiento no autorizado — El daño, la alteración o modificación no autorizada
	Informar al titular		De las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares
	Información mínima		I. La naturaleza del incidente II. Los datos personales comprometidos III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses IV. Las acciones correctivas realizadas de forma inmediata V. Los medios donde puede obtener más información al respecto
	Medidas correctivas por el responsable		— Deberá analizar las causas por las cuales se presentó — Implementará las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, con el fin de evitar que la vulneración se repita
Confidencialidad	Por	— El responsable — Terceros que intervengan en cualquier fase del tratamiento	
	Plazo	Subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable	

Fuente: Miguel Recio Gayo (2013), *Esquemas de la Ley de Protección de Datos Personales y su Reglamento*, México, Tirant lo Blanch, pp. 43-46.

2.3. Normatividad sectorial o específica sobre la protección de datos personales

En materia de protección de datos personales en el ámbito de las telecomunicaciones e Internet, la normatividad sectorial o específica es la LFTR así como, en su caso, otras normas que la desarrollan o complementan.

En concreto, la LFTR es consecuencia de las reformas que se llevaron a cabo en México[45] y es específica, ya que concreta algunos aspectos en relación con la protección de los datos personales y la privacidad en el sector de las telecomunicaciones e Internet.

Y la reforma constitucional en materia de telecomunicaciones[46] tenía por objeto, entre otros, impulsar el bienestar de los usuarios y fomentar el desarrollo económico y social de México.

Al mencionar que se trata de una norma sectorial o específica en materia de protección de datos personales y privacidad, esto significa que los principios, deberes y derechos que se aplican con carácter general a todo tratamiento de datos personales son los previstos en la normatividad general, es decir, la LFPDPPP y su Reglamento, de manera que la LFTR, como normatividad específica, puede concretar algunos aspectos por lo que se refiere a aquellos principios, deberes y derechos.[47]

La LFTR, con carácter general, se remite a la LFPDPPP al referirse en particular a la obligación de los concesionarios de telecomunicaciones y,

[45] En general, sobre las reformas llevadas a cabo en diferentes sectores en México, pueden verse en <http://reformas.gob.mx>, y en particular, en materia de telecomunicaciones, véase la información disponible en <http://reformas.gob.mx/reforma-en-materia-de-telecomunicaciones/que-es>.

[46] Véase el Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6, 7, 27, 28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos, en materia de telecomunicaciones. Disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013>.

[47] En este sentido, aunque referido a la ya abrogada Ley Federal de Telecomunicaciones de 1995 y tomando en consideración el ejemplo de la Unión Europea, puede verse a Julio César Vega Gómez y Miguel Recio Gayo, "La protección de datos en el ámbito de las telecomunicaciones e Internet", *La protección de datos personales en* México, México, Tirant lo Blanch, 2013, p. 413.

en su caso, de los autorizados, de conservar un registro y control de comunicaciones, al indicar que "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" (último párrafo de la fracción II del artículo 190).

Y también, al tratar los derechos de los usuarios, indica la LFTR, en la fracción II de su artículo 191, que éstos tienen derecho "a la protección de los datos personales en términos de las leyes aplicables".

Esta referencia debe entenderse hecha tanto a la normatividad general en materia de protección de datos personales (la LFPDPPP y su Reglamento), como aquéllas otras normas que, en su caso, resulten aplicables, al ser el usuario de los correspondientes servicios de telecomunicaciones un consumidor.

Como consumidor, es necesario tomar en consideración que el usuario quedará también protegido por la Ley Federal de Protección al Consumidor (LFPC).[48] En concreto, un concesionario de telecomunicaciones tendrá que garantizar también al usuario un uso adecuado de sus datos personales cuando contrate sus servicios en virtud de la normatividad en materia de consumo, ya que la LFPC incluye, entre sus principios básicos en las relaciones de consumo, el relativo a "la real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados" (fracción VIII del artículo 1).[49]

[48] Publicada en el *Diario Oficial de la Federación* el 24 de diciembre de 1992. Disponible, con sus sucesivas reformas, en <http://www.diputados.gob.mx/LeyesBiblio/pdf/113_040614.pdf>.

[49] Esta fracción fue adicionada en virtud del Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor, publicado en el *Diario Oficial de la Federación* el 29 de mayo de 2000 y disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/lfpc/LFPC_ref06_29may00.pdf>. Además, la fracción fue modificada por el Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Federal de Protección al Consumidor, publicado en el *Diario Oficial de la Federación* el 4 de febrero de 2004, disponible en <http://www.

Los derechos que se reconocen al usuario de servicios de telecomunicaciones quedarán, por lo tanto, protegidos en virtud de lo previsto también en la LFTR y de la LFPC. Al respecto, la LFTR, en su artículo 191, indica que "los concesionarios y autorizados deberán entregar a los usuarios una carta que contenga los derechos que esta Ley y la Ley Federal de Protección al Consumidor reconocen".

En el desarrollo del artículo 191 de la LFTR, hay que mencionar la publicación de la Carta de Derechos Mínimos de los Usuarios de los Servicios Públicos de Telecomunicaciones, en virtud del Acuerdo mediante el cual la Procuraduría Federal del Consumidor (Profeco) y el Instituto Federal de Telecomunicaciones (IFT), determinan los derechos mínimos que deben incluirse en la carta a que hace referencia el artículo 191 de la Ley Federal de Telecomunicaciones y Radiodifusión.[50]

En concreto, en materia de privacidad y protección de datos personales, la Carta de Derechos Mínimos de los Usuarios de los Servicios Públicos de Telecomunicaciones indica lo siguiente:

> **VII. Derecho a la privacidad y a la protección de datos personales**
>
> **26. Protección de tus datos personales.**
>
> **Tú tienes derecho** a que el proveedor resguarde y proteja tu información personal, como tu nombre, domicilio, correo electrónico, número telefónico y otros.[51]

diputados.gob.mx/LeyesBiblio/ref/lfpc/LFPC_ref10_04feb04.pdf>, y por el Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal; del Código Federal de Procedimientos Penales; de la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes; de la Ley General de Educación; de la Ley de Asociaciones Religiosas y Culto Público; de la Ley Federal de Protección al Consumidor; y de la Ley Reglamentaria del Artículo 5 Constitucional relativo al ejercicio de las profesiones en el Distrito Federal, publicado en el *Diario Oficial de la Federación* el 19 de agosto de 2010 y disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/lfpc/LFPC_ref15_19ago10.pdf>.

[50] Publicado en el *DOF* el 6 de julio de 2015. Disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5399492&fecha=06/07/2015>.

[51] Art. 191 fracción II de la LFTR. Tal y como se cita en la nota a pie de página que aparece en el *DOF* con el número 54.

Asimismo, tiene la obligación de informarte qué datos recaba de ti y con qué fines los utilizará a través de un aviso de privacidad. Tienes derecho a que los datos que proporcionaste sean usados únicamente para los fines que autorizaste y en todo momento, tienes derecho a la seguridad del resguardo de los mismos.[52]

En cualquier caso, puedes acceder, rectificar, cancelar tu información y oponerte a su uso, lo cual se conoce comúnmente como "Derechos ARCO".[53]

En caso de pérdida o daño causado a tus datos personales, el proveedor debe notificarte.[54]

27. Protección de tus comunicaciones y los datos que las identifiquen.

Tú tienes derecho a que el proveedor resguarde y proteja tus comunicaciones, así como los datos que identifiquen las mismas, tales como fecha, hora y duración de las llamadas, mensajes o datos que identifiquen el origen y destino de éstos, entre otros, garantizando su confidencialidad y privacidad.[55]

28. A no recibir llamadas o mensajes de promociones comerciales no autorizadas.

Tú tienes derecho a no recibir llamadas de tu proveedor o de cualquier otro, para promover o vender servicios o paquetes, a menos que expresamente manifiestes tu consentimiento.[56]

[52] Art. 16 y 19 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (en lo sucesivo, LFPDPPP). Tal y como se cita en la nota a pie de página que aparece en el *DOF* con el número 55.

[53] Art. 22 de la LFPDPPP. Tal y como se cita en la nota a pie de página que aparece en el *DOF* con el número 56.

[54] Art. 19 y 20 de la LFPDPPP. Tal y como se cita en la nota a pie de página que aparece en el *DOF* con el número 57.

[55] Art. 190 fracción II de la LFTR. Tal y como se cita en la nota a pie de página que aparece en el *DOF* con el número 58.

[56] Art. 191 fracción XIX de la LFTR. Tal y como se cita en la nota a pie de página que aparece en el *DOF* con el número 58.

Por lo tanto, el IFT, en ejercicio de sus atribuciones y en coordinación con la Profeco, ha determinado que los derechos mínimos de los usuarios de los servicios públicos de telecomunicaciones en materia de privacidad y protección de datos personales son los relativos a:

1. Derecho a la protección de datos personales por el proveedor de servicios públicos de telecomunicaciones, en los términos previstos en la LFPDPPP, a la que se remite la carta;

2. Derecho a la confidencialidad de las comunicaciones y la privacidad de los datos que las identifiquen, en los términos previstos en la LFTR, y

3. Derecho a no recibir llamadas o mensajes promocionales comerciales no autorizadas, también en los términos previstos en la LFTR.

Es necesario considerar la carta como lo que es, una enumeración de derechos mínimos que se enuncian de manera básica, por lo que hay que atender a la normatividad aplicable en cada caso, así como un posible desarrollo de los mismos a través de los instrumentos que resulten oportunos y adecuados, tales como normatividad de desarrollo, esquemas de autorregulación vinculante, etc. Y sin perjuicio del carácter básico y mínimo, habrá que concretar también en la práctica cómo se aplica la previsión relativa a la notificación al titular de los datos en caso de pérdida o daño: ¿qué pérdida o daño?, ¿cuándo?, ¿cómo?, ¿a quién?, ¿qué se notifica?, son sólo algunos de los interrogantes que pueden plantearse. Y, sobre todo, todas las pérdidas o daños, o ¿sólo las "que afecten de forma significativa los derechos patrimoniales o morales de los titulares" (art. 20 de la LFPDPPP)?

En materia de privacidad en relación con la prestación del servicio de acceso a Internet por los concesionarios y autorizados, la LFTR indica también, en su artículo 145, que entre los principios a que deberán sujetarse los lineamientos que emita el IFT, está el de privacidad, de manera que "deberán preservar la privacidad de los usuarios y la seguridad de la red".

Una cuestión específica que debe tomarse en consideración en relación con lo anterior es la obligación de los concesionarios de servicios de telecomunicaciones de colaborar con la justicia. Es ésta, además, una materia que debe ser desarrollada a través de lineamientos del IFT, pudiendo señalar que en 2014 se llevó a cabo por dicho Instituto una consulta pública sobre el anteproyecto de lineamientos de colaboración de la justicia.[57]

[57] La referencia a la consulta pública, entre el 12 y el 27 de noviembre de 2014, puede verse en <http://www.ift.org.mx/iftweb/industria-2/industria-intermedia-nv/consulta-publica-del-anteproyecto-de-lineamientos-de-colaboracion-en-materia-de-seguridad-y-justicia>. El Anteproyecto de Lineamientos de Colaboración en Materia de Seguridad y
Justicia se publicó en <http://www.ift.org.mx/iftweb/wp-content/uploads/2014/11/Anteproyecto_Lineamientos_Colaboracion_Seguridad.pdf>. Los comentarios recibidos por la IFT fueron publicados en <http://www.ift.org.mx/iftweb/categoria/consultas_publicas/consulta-publica-lineamientos-de-colaboracion-en-materia-de-seguridad-y-justicia>.

3. ALGUNAS CONSIDERACIONES SOBRE EL USUARIO DE TELECOMUNICACIONES E INTERNET

Cuando el usuario, persona física, utiliza los servicios de telecomunicaciones proporcionados por un concesionario de telecomunicaciones o autorizado sujeto a la normatividad mexicana, sus datos personales tienen que ser protegidos por estos sujetos ya que están obligados a cumplir tanto con la normatividad general sobre protección de datos como con la normatividad sectorial o específica. En este sentido, el usuario de servicios de telecomunicaciones es el titular de los datos personales.

Que los datos personales del usuario de telecomunicaciones sean protegidos conforme a la normatividad aplicable es tanto una obligación de los sujetos obligados para garantizar el derecho fundamental a la protección de datos como una medida que ayuda a fomentar la confianza de los titulares de los datos en el uso de la tecnología y los servicios de telecomunicaciones.

Sin perjuicio de lo anterior, el usuario de servicios de telecomunicaciones e Internet también tiene obligaciones como la de hacer un uso responsable de la tecnología, de manera que proteja sus datos personales y otra información con el fin de evitar riesgos. Es importante, por lo tanto, que el usuario sea consciente del valor de sus datos personales y de las implicaciones que puede tener para el mismo hacer uso de servicios sin leer previamente los términos y condiciones, especialmente por lo que se refiere al tratamiento y uso de los datos personales que va a proporcionar. Además, adoptar medidas para proteger sus datos personales y privacidad es importante, pudiendo hacer uso a tal fin de la tecnología y de los servicios disponibles (resumen del capítulo elaborado por el autor del ensayo).

3.1. Garantizar el derecho fundamental a la protección de datos del usuario

El usuario[58] de servicios de telecomunicaciones e Internet, cuando se trata específicamente de una persona

[58] En relación con este concepto, la LFTR define en la fracción LXXI de su artículo 3 al usuario final como "persona física o moral que utiliza un servicio de telecomunicaciones como destinatario final".

física, requiere de protección con la finalidad de garantizar su derecho fundamental a la protección de datos personales y, por lo tanto, de evitar la vulneración o intromisión ilegítima en sus derechos.

Este usuario, persona física, es titular de derechos en virtud de la normatividad que regula las telecomunicaciones y, además, es titular de los datos personales[59] que hacen referencia al mismo y que le identifican o permiten identificarle.[60] A pesar de que la normatividad aplicable tanto en materia de telecomunicaciones como de protección de datos personales, por las competencias, es la federal, cabe prestar también atención a la definición de datos personales de la normatividad del Distrito Federal, ya que la misma puede aportar criterios y elementos a considerar a la hora de determinar quién es el titular de los datos y qué datos personales son o pueden estar siendo tratados.

Un dato relevante que hay que considerar en este sentido es que "a diario en la Ciudad de México, las personas proporcionan al menos 35 veces sus datos personales, sin tener conciencia de que deben estar protegidos y no deberán ser utilizados con fines distintos por los cuales fueron entregados".[61]

Hay que tener en consideración también que el usuario es la persona física que "utiliza un servicio de telecomunicaciones como destinatario final",[62] de manera que no se identifica necesariamente con el suscriptor;

[59] Al que se define en la fracción XVII del artículo 3 de la LFPDPPP como "la persona física a quien corresponden los datos personales".

[60] Por lo que se refiere al concepto de datos personales, son definidos por el artículo 2 de la Ley de Protección de Datos Personales para el Distrito Federal como "La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos." Publicada en la *Gaceta Oficial del Distrito Federal* el 3 de octubre de 2008 y disponible en <http://www.infodf.org.mx/nueva_ley/14/1/doctos/LPDPDF.doc>.

[61] Comunicado de prensa del InfoDF, 15 de octubre de 2014. Disponible en <http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=2084&Itemid=217>.

[62] Según la definición dada en la fracción LXXI del artículo 3 de la LFTR.

es decir, quien tiene un contrato con el concesionario, lo que implica que si por ejemplo una línea de telefonía fija fuese utilizada por otras personas que conviven con el suscriptor, por ejemplo, un hijo o una hija, serán también usuarios finales y por lo tanto quedarán protegidos por la normatividad aplicable, tanto general como sectorial o específica, en materia de protección de datos personales y privacidad.

En definitiva, el usuario, persona física y titular de los datos personales, es quien debe tener garantizado su derecho fundamental a la protección de datos personales tanto en virtud de la normatividad general, en materia de protección de datos personales, como de la sectorial o específica, en el sector de las telecomunicaciones y, en su caso, sobre protección de los consumidores.

3.2. ¿Cómo se consigue una protección efectiva?

La protección efectiva del usuario de servicios de telecomunicaciones o, en su caso, de Internet o servicios relacionados con Internet, requiere que todas las partes interesadas e involucradas, desde el legislador hasta las organizaciones de la sociedad civil, ejerzan sus competencias con la finalidad de conseguir un alto nivel de protección de datos personales y privacidad.

Garantizar la protección de datos personales, la privacidad y otros derechos es una cuestión clave también para generar la confianza necesaria[63] en el uso de servicios de telecomunicaciones e Internet.

Al respecto, la normatividad desempeña un papel relevante por lo que se refiere al reconocimiento de los derechos de los usuarios, desarrollando en su caso las previsiones de la Constitución, si bien dicha

[63] En este sentido, por ejemplo, la comisionada presidenta del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Ximena Puente de la Mora, durante su participación en un seminario internacional que tuvo lugar en Santiago de Chile, en diciembre de 2014, manifestó que "el desarrollo tecnológico plantea serios y crecientes desafíos para la protección de los datos personales". Véase la nota de prensa del INAI en <http://inicio.ifai.org.mx/Comunicados/Comunicado%20IFAI-163-14.pdf>. El IFAI cambió su denominación en virtud del Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública, publicada en el *DOF* el 4 de mayo de 2015. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf>.

protección debe ser complementada con otras medidas por las diferentes partes involucradas en la prestación de servicios de telecomunicaciones e Internet, tales como la autorregulación y el desarrollo tecnológico que incorpore la privacidad por diseño y por defecto, manteniéndola a lo largo del tiempo y del tratamiento de los datos personales.

Entre otras medidas, la autorregulación debe ser tomada en consideración como un instrumento adecuado para proteger al usuario de servicios de telecomunicaciones e Internet que, al mismo tiempo, es titular de datos personales. Es así que todo esquema de autorregulación en la materia, además de ser vinculante, tiene que garantizar un nivel de protección superior al que otorga la normatividad, pudiendo ser también el instrumento idóneo para promover buenas prácticas en este sector específico.

Cuando dichos esquemas de autorregulación incluyan aspectos relativos a la protección de datos personales, se deberán tener en consideración los Parámetros de Autorregulación en Materia de Protección de Datos Personales y, en su caso, la inscripción de dichos esquemas en el Registro de Esquemas de Autorregulación (REA) del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI),[64] la cual se producirá siempre y cuando cumplan con los requisitos establecidos en los citados parámetros.[65]

Además, la protección efectiva requiere también que el propio usuario conozca y ejerza sus derechos, de manera responsable. Es decir, el usuario debe ser consciente también de cuándo, a quién y para qué da sus datos personales. Y también debe considerar las consecuencias de sus acciones, especialmente en línea (*online*), cuando por ejemplo comparte fotografías en redes sociales o publica datos personales en páginas web, en foros, o acepta solicitudes para agregar a otros usuarios en diversas redes.

Al publicar o compartir datos personales, incluidas las fotografías, en

[64] Para obtener más información véase <http://www.rea.ifai.org.mx/_catalogs/masterpage/Sec1_1.aspx>.

[65] Tal y como concreta el artículo 86 del Reglamento de la LFPDPPP, relativo al registro de esquemas de autorregulación.

la web o en una red social, no sabemos quién puede llegar a verlos y cómo puede utilizarlos. Por ejemplo, dar información sobre nuestras próximas vacaciones en una red social podría ser una valiosa información de que dejamos sola nuestra casa durante un tiempo; las fotografías hechas en el antro y compartidas en la red social podrían tener importancia en un proceso de selección para un trabajo; al aceptar una invitación de un desconocido en una red le podemos estar compartiendo información que no sabemos con qué fines utilizará e incluso facilitando el acceso al perfil de nuestros amigos, y cualquier otra información que se proporcione sin un debido cuidado, puede ser usada por un estafador con el objetivo de obtener más datos o incluso conseguir el acceso a nuestra cuenta bancaria. Por lo tanto, es necesario ser conscientes de que hacer uso de la tecnología conlleva importantes ventajas pero debe hacerse con cuidado, sin dar más datos personales de los necesarios o activando los controles de privacidad que se nos ofrecen o que tenemos a nuestra disposición.

3.3. El usuario también tiene obligaciones

El usuario de servicios de telecomunicaciones, y en particular de Internet, tiene que hacer uso responsable de los mismos, de manera que antes de dar datos personales o permitir el acceso a aplicaciones (en inglés, *apps*) a sus dispositivos y datos personales, se asegure de haber leído y comprendido el correspondiente aviso de privacidad o tome una decisión sobre el uso, o no, de un servicio o una aplicación en caso de que este aviso de privacidad no sea proporcionado.

Las obligaciones que tiene el usuario también se refieren a sus acciones, especialmente por lo que se refiere al uso de Internet o servicios tales como las redes sociales, el correo electrónico o la publicación de blogs.

El caso de la catequista sueca que publicó datos personales en Internet

En la Unión Europea, la primera vez que el Tribunal de Justicia de la Unión Europea (TJUE)[66] se pronunció en materia de protección

[66] Sobre el TJUE puede verse más información en <http://curia.europa.eu/jcms/jcms/

de datos fue en 2001, en el caso[67] de una catequista sueca, la sra. Lindqvist, que había publicado datos personales de sus compañeros en Internet.

En este caso, el TJUE dio respuesta a una petición de decisión prejudicial planteada por el Göta hovrätt (un órgano jurisdiccional sueco ante el que se siguió un proceso penal contra la persona ya mencionada) sobre la interpretación de la Directiva 95/46/CE,[68] ya que el Eksjö tingsrätt (tribunal sueco) condenó a la sra. Lindqvist al pago de una multa como consecuencia de haber tratado datos personales incumpliendo los principios de la citada Directiva que habían sido transpuestos al ordenamiento jurídico sueco a través de la correspondiente ley nacional.

En concreto, la sra. Lindqvist hizo un curso de informática en el que se requería que creara una página web. Es así que en su casa, utilizando su equipo de cómputo personal, creó una página web en la que incluyó datos personales de sus compañeros y pidió al administrador de la página web de su parroquia incluir una liga a su página web para que así los feligreses pudieran encontrar fácilmente dicha información.

Entre los datos personales que la sra. Lindqvist incluyó en la web se encontraba el nombre completo, o a veces sólo el nombre, de sus compañeros; sus funciones, en ocasiones descritas con un poco de

Jo2_7024>.

[67] Véase la Sentencia del Tribunal de Justicia del 6 de noviembre de 2003, "Directiva 95/46/CE – Ámbito de aplicación – Publicación de datos personales en Internet – Lugar de la publicación – Concepto de transferencia de datos personales a países terceros – Libertad de expresión – Compatibilidad con la Directiva 95/46 de una protección más rigurosa de los datos personales por parte de la normativa de un Estado miembro", en el asunto C-101/01. Disponible en <http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=337168>.

[68] Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. Publicada en el *Diario Oficial de la Unión Europea*, núm. L 281, 23 de noviembre de 1995. Disponible en <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&qid=1421355094859&from=ES**>.**

humor; sus aficiones; en algunos casos su situación familiar; su número de teléfono y otra información personal. Además, en el caso de una compañera de parroquia, hizo referencia a que se había lesionado un pie y que estaba de baja parcial por enfermedad, lo que suponía que fuese un dato sensible por referirse a la salud de una persona.

Al incluir esta información en la página web que había creado, lo hizo sin informar ni obtener el consentimiento necesario de sus compañeros, lo que suponía una infracción de la Ley Sueca sobre Protección de Datos.

Además, este tratamiento de datos personales no podía ampararse en la excepción relativa al tratamiento de datos "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas",[69] ya que como indica el TJUE "esta excepción debe interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es éste el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas".[70]

Esta acción, consistente en crear una página web y tratar datos personales en la misma, sin informar ni obtener el consentimiento necesario, además de otras obligaciones conforme a la Ley Sueca sobre Protección de Datos, supuso la comisión de una infracción, de manera que la sra. Lindqvist tuvo que pagar una multa económica y, además, verse sometida a un proceso penal (resumen del caso elaborado por el autor del ensayo).

El caso de la sra. Lindqvist sirve para ilustrar que el usuario tiene que adoptar medidas para proteger tanto sus datos personales y su privacidad, así como la de terceros, en Internet y en otros servicios electrónicos, como por ejemplo en las redes sociales.

[69] Véase el segundo guión del artículo 3, apartado 2, de la Directiva 95/46/CE.

[70] Apartado 47 de la sentencia del TJUE.

En definitiva, el usuario tiene que hacer uso responsable de la tecnología y de los servicios, en particular cuando hay algunos que se ofrecen etiquetados como "gratuitos", pero que en la práctica pueden implicar que se pague los mismos con sus datos personales.[71] Es por ello que el usuario es una de las partes interesadas e involucradas en la protección de sus datos personales y privacidad, de manera que debe ser consciente de que tiene un derecho fundamental, así como conocer su significado y alcance, para ejercerlo.

[71] En este sentido, puede verse "Supervisor Europeo de Protección de Datos (2014)", *Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital economy*. Disponible en inglés en <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf>.

4. LA PROTECCIÓN DE DATOS PERSONALES EN LAS TELECOMUNICACIONES

Al hacer uso de servicios de telecomunicaciones se produce o puede producir un tratamiento de datos personales, relativos al usuario de dichos servicios, que tiene que cumplir tanto con la normatividad general como sectorial o específica en materia de protección de datos personales. Este tratamiento de datos personales se produce al hacer uso de los diferentes servicios de telecomunicaciones disponibles, tales como la telefonía fija o móvil e Internet.

Si bien la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) no establece un listado de los datos personales específicos que se tratan en cada caso, hay que atender a la definición misma de datos personales, entendidos como cualquier información relativa a una persona identificada o identificable, además de tener en consideración la normatividad específica, como por ejemplo la que desarrolla lo relativo a los registros que deben conservar los concesionarios de telecomunicaciones para cumplir con las obligaciones que les impone la normatividad aplicable.

Los fines con los que dichos concesionarios de telecomunicaciones o, en su caso, autorizados, pueden tratar los datos personales de los usuarios tienen que cumplir, en todos los casos, con los principios, deberes y derechos previstos en la normatividad sobre protección de datos personales. No obstante, hay que distinguir entre fines para los que se requiere el consentimiento del usuario, como titular de los datos personales, pudiendo citar como ejemplo el envío de publicidad o las llamadas con dicha finalidad, y fines que no requieren de dicho consentimiento, por estar previstos en la ley o ser necesarios para cumplir con la relación contractual entre el concesionario y el usuario, como por ejemplo la prestación del servicio o el cumplimiento de obligaciones legales relativas a conservar un registro de comunicaciones en los términos previstos en la ley.

En cualquier caso, los concesionarios de telecomunicaciones y autorizados tienen que cumplir con la normatividad sobre protección de datos personales, garantizando así el derecho fundamental a la protección de datos personales de los usuarios como titulares del mismo (resumen del capítulo elaborado por el autor del ensayo).

4.1. Servicios de telecomunicaciones

Las telecomunicaciones[72] incluyen diversos servicios a través de las cuales los usuarios se pueden comunicar, ya que es posible enviar o emitir y recibir signos, imágenes, sonidos y cualquier otro tipo de datos, a través de canales de transmisión como el cable, la fibra óptica o el espectro radioeléctrico.

Una llamada de voz, el envío de un mensaje de texto o SMS (en inglés, *Short Message System*) o la conexión para el acceso a Internet, son servicios de telecomunicaciones que se usan a diario o casi a diario con fines de comunicación e interactuar con otras personas u organizaciones, públicas o privadas.

En todos estos servicios de telecomunicaciones se produce un tratamiento de datos personales[73] del usuario que, en su caso, son parte de la comunicación. Este tratamiento tiene que cumplir con la normatividad aplicable, tanto general como sectorial o específica, en materia de protección de datos personales, además de que se garanticen también otros derechos fundamentales, como el derecho a la inviolabilidad o secreto de las comunicaciones.

También hay supuestos, tales como el ejercicio del derecho a la portabilidad, o servicios de valor agregado basados en la geolocalización, que implican un tratamiento de datos personales de los usuarios.

[72] Véase la definición de telecomunicaciones en la fracción LXVIII del artículo 3 de la LFTR.

[73] Por tratamiento de datos personales, conforme a la definición dada en la fracción XVIII de la LFPDPPP, se entiende "la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales".

En unos casos, como ocurre con la portabilidad, el tratamiento de los datos personales estará previsto en la ley de manera que no es necesario el consentimiento del titular de los datos; mientras que en otros casos, como ocurre con algunos servicios de geolocalización, sí será necesario el consentimiento del titular de los datos personales para poder tratarlos lícitamente, sin perjuicio de que dicho tratamiento tenga que cumplir también con el resto de principios aplicables.

Las telecomunicaciones son, por lo tanto, un claro ejemplo de uso de las tecnologías de la información y las comunicaciones (TIC) que hace posible la comunicación, así como el acceso a la información y los servicios electrónicos, siendo necesario garantizar un tratamiento legítimo, controlado e informado, con la finalidad de generar la confianza necesaria en su uso y el respeto al derecho fundamental a la protección de datos personales.

4.2. ¿Qué datos personales se tratan en los servicios de telecomunicaciones?

En cuanto a qué datos personales manejan los concesionarios que prestan servicios de telecomunicaciones, se puede prestar atención, de manera orientativa, a la fracción II del artículo 190 de la LFTR.

Este artículo incluye un listado de los datos personales que tratarán los concesionarios de telecomunicaciones y, en su caso, los autorizados, ya que tienen la obligación legal de "conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad".

En concreto, los registros que tratan los concesionarios de telecomunicaciones deberán permitir identificar los siguientes datos personales:

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.

Si bien este listado indica qué datos personales se tratan por parte de los concesionarios de telecomunicaciones y, en su caso, los autorizados para el cumplimiento de las obligaciones en materia de seguridad y justicia, permite saber qué datos personales son objeto de tratamiento en la prestación de los servicios de telecomunicaciones mencionados. No obstante, los servicios específicos y los fines concretos para los que se traten, en cada caso, los datos personales, pueden implicar que haya que agregar a dicho listado otros datos personales.

Este listado genérico de datos personales relativos a las telecomunicaciones, ya sea telefonía fija, móvil o comunicaciones basadas en el

protocolo IP,[74] es desarrollado y concretado por el Anteproyecto de Lineamientos de Colaboración en Materia de Seguridad y Justicia.

En concreto, el Lineamiento décimo tercero, incluido dentro del capítulo IV, relativo al registro de datos de comunicaciones, hace referencia a la ya citada fracción II del artículo 190 de la LFTR e indica que: "el sistema o sistemas utilizados para el registro de datos de comunicaciones de líneas privadas, telefonía fija y móvil y comunicaciones que utilicen el protocolo IP, deberá contar con la capacidad de almacenar y entregar los datos" relativos a:

I. Para líneas privadas, se registrarán y conservarán los datos correspondientes al nombre del usuario registrado, la dirección de origen y destino de la línea.

II. Para telefonía fija, se registrará y conservará la información correspondiente a:

a) Nombre y dirección del usuario registrado;
b) Tipo de comunicación;
c) Números de origen y destino; y
d) Duración, fecha y hora de la comunicación.

III. Para telefonía móvil en las modalidades de prepago y pospago se registrará y conservará la información correspondiente a:

a) Nombre y dirección del usuario registrado, en el caso de la modalidad de pospago;
b) Tipo de comunicación;

[74] El protocolo IP es el protocolo de comunicación utilizado en Internet que se basa en direcciones IP. Estas direcciones IP, son numéricas y tienen la forma A.B.C.D, teniendo cada uno de estos elementos un valor entre 0 y 255. Por ejemplo, la dirección IP del InfoDF es 200.76.41.226, estando asociada al nombre del dominio infodf.org.mx, de manera que no es necesario recordar dicha dirección IP. Una explicación básica del funcionamiento de Internet y algunos conceptos básicos, puede verse en el documento del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, titulado *Documento de trabajo Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea*, WP 37, adoptado el 21 de noviembre de 2000. Disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_es.pdf>.

c) Los números de origen y destino;
d) Duración, fecha y hora de la comunicación;
e) Fecha y hora de la primera activación del servicio;
f) La etiqueta de localización (identificador de celda) desde la que se haya activado el servicio por primera vez;
g) IMEI (del inglés *International Mobile System Equipment Identity*, Identidad de Equipo del Internacional Sistema Móvil); y
h) IMSI (del inglés *International Mobile Subscriber Identity,* Identidad Internacional del Abonado a un teléfono móvil).

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

a) El lugar, fecha y hora en la que se realizó la compra del dispositivo de prepago o la tarjeta SIM, en el caso en que el concesionario o autorizado los comercialice por canales propios, o

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

V. Para comunicaciones que empleen el protocolo IP se registrará y conservará:

a) El nombre, denominación o razón social y dirección del usuario al que en el momento de la comunicación se le haya asignado una dirección IP;
b) El tipo de comunicación (el servicio de Internet utilizado);
c) Usuarios registrados destinatarios de la comunicación;
d) Fecha y hora de la comunicación IP basada en un determinado huso horario;
e) La dirección IP, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet; y
f) Tiempo durante el cual estuvo asignada dicha dirección IP.[75]

[75] En cuanto a las siglas IMEI e IMSI, conforme a las definiciones incluidas en el lineamiento segundo del Anteproyecto de Lineamientos, se entiende por IMEI el "Código de identidad de fabricación del equipo, por sus siglas en inglés, *International Mobile Equipment Identity Number*" (fracción X), y por IMSI el "Código de identidad internacional del usuario móvil, por sus siglas en inglés, *International Mobile Subscriber Identity*".

Por lo tanto, los datos personales que pueden tratarse, en su caso, en los diferentes servicios de telecomunicaciones, ya sea telefonía fija o móvil, en la modalidad de prepago o pospago, o en comunicaciones basadas en el protocolo IP, entran dentro del concepto de datos personales de la LFPDPPP en la medida en que identifican o permiten identificar al usuario que es persona física y titular de dichos datos.

En relación con el titular de los datos personales, es necesario poner atención al concepto de persona física identificable, siendo definida por el Reglamento de la LFPDPPP como "toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas" (fracción VIII del artículo 2).

Es así que, por ejemplo, el número de teléfono de un usuario que sea persona física y titular de datos personales, será considerado un dato personal. Por su parte, el número de teléfono de una empresa no será considerado como un dato personal, sin perjuicio de los derechos que correspondan a dicha empresa como usuario de servicios de telecomunicaciones.

Sin perjuicio de lo anterior, es necesario distinguir entre los datos relativos a las partes de la comunicación y el contenido de la comunicación. En el primer caso, se puede tratar de datos personales en los términos ya expuestos y, por lo tanto, su titular queda protegido por el derecho fundamental a la protección de datos personales en virtud de la normatividad general y sectorial o específica en la materia. En el segundo caso, el contenido de la comunicación, ya sea voz o datos, queda protegido por el derecho fundamental al secreto o la inviolabilidad de las comunicaciones.

4.3. ¿Para qué se tratan los datos personales?

Los datos personales de los usuarios que sean personas físicas, de servicios de telecomunicaciones, pueden utilizarse con diferentes finalidades y, en cualquier caso, dichos tratamientos de datos tienen que llevarse a cabo con apego a la normatividad general y específica o sectorial en la materia.

Es así que los datos personales en relación con los servicios de telecomunicaciones pueden tratarse por los concesionarios de telecomunicaciones y, en su caso, los autorizados, con diversas finalidades. Entre otras, podrían identificarse fines relativos a:

— la prestación del servicio de telecomunicaciones;
— la prestación de servicios de valor agregado;
— la facturación y cobranza del servicio correspondiente;[76]
— gestionar la portabilidad del número de usuario;
— la elaboración de directorios telefónicos;
— realizar investigaciones y monitoreos sobre el comportamiento crediticio del suscriptor;
— prevenir el fraude en la contratación;
— mercadotecnia, publicidad o prospección comercial; o
— cumplir con las obligaciones en materia de seguridad y justicia.

Al respecto, sobre algunos de estos y otros servicios, la LFTR prevé, en su artículo 136 que el IFT "establecerá y garantizará, a través de la publicación de normas, las medidas conducentes y económicamente competitivas, para que los usuarios de todas las redes públicas de telecomunicaciones puedan obtener acceso a servicios de facturación, información, de directorio, de emergencia, de cobro revertido y vía operadora, entre otros". Por lo tanto, habrá que prestar atención, en su caso, a las normas del IFT en cuanto a los servicios de facturación, información y de directorio, entre otros, ya que todos estos servicios implican un tratamiento de datos personales en el caso de usuarios que son personas físicas.

En relación con estas finalidades es necesario distinguir entre las primarias y las secundarias, ya que de ello depende cómo cumplir con determinados principios de la protección de datos personales. Es así que, por ejemplo, un concesionario de telecomunicaciones no necesita obte-

[76] Por lo que se refiere a la cobranza extrajudicial, puede tomarse en consideración la publicación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2015), *Guía para orientar el debido tratamiento de datos personales en la actividad de cobranza extrajudicial*. Disponible en <http://inicio.ifai.org.mx/DocumentosdeInteres/Guía_Cobranza_Extrajudicial_IFAI.pdf>.

ner el consentimiento del usuario de sus servicios, que es el titular de los datos personales, para brindarle el servicio contratado, pero sí tendrá que obtener su consentimiento para utilizar sus datos personales con fines de publicidad o prospección comercial.

El tratamiento de datos personales de un suscriptor, persona física, con una finalidad primaria, que es necesaria para el cumplimiento de la relación contractual que tiene por objeto la prestación del servicio o una finalidad prevista en la ley, no requiere del consentimiento del titular de los datos. En este sentido, son aplicables las excepciones al consentimiento previstas para el tratamiento de los datos personales en el artículo 10 de la LFPDPPP,[77] entre las que se encuentran las anteriores.

En el caso de que los datos personales de los suscriptores fueran a ser utilizados por el concesionario de telecomunicaciones, por ejemplo, para enviar publicidad sobre nuevos servicios o hacer una investigación de mercado que le permita ofrecer nuevos productos o servicios a sus suscriptores o a nuevos clientes, personas físicas, en dicho caso los suscriptores requerirán obtener el consentimiento necesario para ello.

Y dicho consentimiento no será necesario, como se ha indicado, por ejemplo, cuando el concesionario de telecomunicaciones o, en su caso, el autorizado, presta el servicio al usuario o también para facturar dicho servicio. Son tratamientos de datos personales previstos en la ley y ade-

[77] El artículo 10 de la LFPDPPP indica que:
Artículo 10. No será necesario el consentimiento para el tratamiento de los datos personales cuando:
I. Esté previsto en una ley;
II. Los datos figuren en fuentes de acceso público;
III. Los datos personales se sometan a un procedimiento previo de disociación;
IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente; o
VII. Se dicte resolución de autoridad competente.

más necesarios para el cumplimiento del contrato entre el concesionario de telecomunicaciones y el suscriptor, de manera que queda excluidos de la necesidad de obtener el consentimiento del suscriptor, como titular de los datos.

En concreto, la facturación del servicio también estaría excepcionada de la necesidad de obtener el consentimiento, porque es un tratamiento previsto en la ley y, por lo tanto, entraría dentro de las excepciones previstas en la normatividad sobre protección de datos personales.

El consentimiento del suscriptor tampoco será necesario para la transferencia, nacional o internacional, de sus datos personales en los casos previstos en la LFPDPPP,[78] por ejemplo, si la misma está prevista en una ley o es necesaria para mantener o cumplir la relación jurídica entre el concesionario o, en su caso, autorizado, como responsables del tratamiento, y el suscriptor, como titular de los datos personales.

Sin perjuicio de lo anterior, dichos tratamientos de datos personales tienen que cumplir con los demás principios aplicables, ya citados anteriormente. Es decir, aunque el consentimiento no sea necesario, el concesionario sí tiene que informar al usuario sobre el tratamiento de sus datos personales a través del correspondiente aviso de privacidad y

[78] En concreto, el artículo 37 de la LFPDPPP indica que:
Artículo 37. Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:
I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

cumplir con los demás principios, deberes y derechos aplicables, en el caso de que utilice los datos personales del suscriptor para prestarle el correspondiente servicio.

Cabe destacar que la LFTR incluye algunas cuestiones específicas, como normatividad sectorial que complementa, en su caso, a la normatividad general sobre protección de datos personales. Así, por ejemplo, se indica que el IFT podrá imponer al agente económico preponderante la obligación de "actuar sobre bases no discriminatorias al proporcionar información de carácter comercial respecto de sus suscriptores, a filiales, subsidiarias o terceros, sin perjuicio de lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (artículo 267).

También la LFTR incluye una referencia específica, relativa a la calidad de los datos personales que trate el concesionario o, en su caso, el autorizado, ya que prevé como infracción "proporcionar dolosamente información errónea de usuarios, de directorios, de infraestructura o de cobro de servicios" [79] (fracción VI del apartado C) del artículo 298).

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tendrán que cumplir también con los deberes de seguridad y confidencialidad, así como adoptar las medidas necesarias y oportunas para gestionar las solicitudes de derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) que reciban.[80]

4.4. Facturación

Un tratamiento de datos específico y relevante es el relativo a la facturación de los servicios de telecomunicaciones.

[79] Sancionable con multa por el equivalente de 1.1% hasta 4% de los ingresos del concesionario o autorizado.

[80] En cuanto a las obligaciones de los concesionarios de telecomunicaciones y, en su caso, autorizados, como responsables del tratamiento, puede verse Instituto Federal de Acceso a la Información y Protección de Datos (2014), *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_julio2014.pdf>.

Al respecto, el suscriptor tiene derecho a la factura por los servicios de telecomunicaciones de los que hace uso y la LFTR indica, en este sentido, que entre las medidas que el IFT podrá imponer al agente preponderante se encuentra la de "desglosar de manera individual y suficiente en las facturas que expida, cada uno de los servicios que presta, con el objeto de conocer las tarifas o precios aplicables a cada uno de ellos" (fracción XV del artículo 267).

Por su parte, el artículo 135 del Reglamento de Telecomunicaciones,[81] que se entiende vigente en tanto se emitan los nuevos ordenamientos de la LFTR[82] que lo sustituyan, y en lo que no se oponga a ésta, indica que "los concesionarios deberán facturar a sus suscriptores el importe por el consumo de los servicios contratados, desglosando el adeudo total en los conceptos originados por cada uno de los servicios utilizados".

Por lo tanto, la facturación es un ejemplo de tratamiento de datos personales que no requiere del consentimiento del usuario, por estar previsto en la ley, si bien tiene que cumplir con el resto de principios que legitiman dicho tratamiento de datos. Además, la facturación, como tratamiento de datos personales, implica que se deba tener en consideración tanto la normatividad general como la sectorial o específica.

4.5. Directorios telefónicos

Por lo que se refiere a los directorios telefónicos, cabe señalar que hay que atender a lo dispuesto en el Reglamento de Telecomunicaciones, de manera que resulta aplicable su artículo 92 en relación con dichos directorios.[83]

---

[81] Publicado en el *Diario Oficial de la Federación* el 20 de octubre de 1990. Disponible, con actualizaciones, en <http://www.ift.org.mx/iftweb/wp-content/uploads/2012/07/78_Reglamento_de_Telecomunicaciones_01.pdf>.

[82] Al respecto, el artículo transitorio tercero de la LFTR indica que "las disposiciones reglamentarias y administrativas y las normas oficiales mexicanas en vigor, continuarán aplicándose hasta en tanto se expidan los nuevos ordenamientos que los sustituyan, salvo en lo que se opongan a la Ley Federal de Telecomunicaciones y Radiodifusión que se expide por virtud del presente Decreto".

[83] En concreto, el artículo 92 del Reglamento de Telecomunicaciones indica lo siguiente: Con excepción de aquellos números que el usuario haya solicitado mantener privados, los concesionarios del servicio público telefónico están obligados a proporcionar un

En virtud de dicho artículo, el suscriptor tiene reconocidos los siguientes derechos:

- A que su número de teléfono se mantenga privado en el servicio de información de directorio telefónico; y

- A una copia, gratuita y anual, del directorio telefónico.

Los datos personales que aparecerán en el directorio telefónico, según indica el Reglamento de Telecomunicaciones, son los relativos a nombre, domicilio y código postal del suscriptor, y el número telefónico que éste tenga asignado.

Estos directorios telefónicos son, además, considerados como fuentes de acceso público[84] en virtud de lo que indica el artículo 7 del Reglamento de la LFPDPPP.[85] Por lo tanto, los datos personales que sean incluidos en

servicio de información de directorio por operadora.
Asimismo, los concesionarios de telefonía básica deberán publicar y distribuir anual y gratuitamente entre sus usuarios, un directorio telefónico que contenga el nombre, domicilio y código postal del suscriptor, y el número telefónico que éste tenga asignado.
Los concesionarios están obligados a incluir en el directorio los números de los suscriptores de otros operadores de redes públicas autorizadas por la Secretaría, siempre y cuando así se lo soliciten y le proporcionen la información respectiva, teniendo la facultad de negociar los términos y condiciones; si no llegaren a un acuerdo escuchando a los interesados, la Secretaría decidirá lo conducente.
Los concesionarios están obligados a atender las solicitudes de información de directorio provenientes de otros operadores de redes públicas interconectadas, nacionales o extranjeros, para fines de información de directorio a los usuarios de dichos operadores, así como las solicitudes de empresas de elaboración y publicación de directorios.
Esta información deberá proporcionarla en la forma y medio en que se le solicite, pudiendo cobrar un cargo por los gastos que representa dicha información en la forma solicitada.

[84] Las fuentes de acceso público son definidas en la fracción X del artículo 3 de la LFPDPPP como "aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación, de conformidad con lo señalado por el Reglamento de esta ley".

[85] Dicho artículo indica, en concreto, lo siguiente:
Fuentes de acceso público
Artículo 7. Para los efectos del artículo 3, fracción X de la ley, se consideran fuentes de acceso público:
I. Los medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;

estos directorios telefónicos podrán tratarse sin necesidad de obtener el consentimiento de su titular, respetando la expectativa razonable de privacidad del titular de los datos personales.

La expectativa razonable de privacidad consiste, tal y como indica el artículo 7 de la LFPDPPP, en "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" en la ley y que está vinculada con el principio de lealtad que implica, a su vez, que, como indica el primer párrafo del artículo 44 del Reglamento de la LFPDPPP, el responsable tenga que "tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad".

4.6. Geolocalización

La geolocalización implica que se puede saber dónde está exactamente una persona que utiliza un celular o un dispositivo de manera que ello permite a los proveedores prestarle servicios de valor agregado, tales como servicios de información, y a los usuarios acceder a múltiples servicios avanzados y basados en dicha geolocalización.[86]

II. Los directorios telefónicos en términos de la normativa específica;
III. Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa; y
IV. Los medios de comunicación social.
Para que los supuestos enumerados en el presente artículo sean considerados fuentes de acceso público, será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contraprestación, derecho o tarifa.
No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.
El tratamiento de datos personales obtenidos a través de fuentes de acceso público, respetará la expectativa razonable de privacidad, a que se refiere el tercer párrafo del artículo 7 de la ley.

[86] En relación con la geolocalización, el Grupo de Trabajo del artículo 29, ya mencionado, ha indicado que "con el rápido desarrollo tecnológico y la amplia difusión de dispositivos móviles inteligentes, se está desarrollando una nueva categoría de servicios basados en la localización". Véase Grupo de Trabajo del artículo 29, *Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes*, WP 185, p. 3. Disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_es.pdf>.

Desde consultar dónde está el restaurante más cercano hasta obtener ayuda, por ejemplo, en un accidente al facilitar a los servicios de emergencia la localización del usuario, son ejemplos de algunos servicios basados en la geolocalización.

En particular, hay tres infraestructuras que permiten prestar servicios de geolocalización: GPS, estaciones de base GSM y WiFi.[87]

Los servicios basados en la geolocalización son un buen ejemplo de lo que permite la innovación y evolución tecnológica, de manera que pueden aportar importantes beneficios, tales como la posibilidad de acceder a información o ayuda en virtud de la localización.

No obstante, dichos servicios tienen que cumplir también con la normatividad aplicable, de manera que en el caso específico de los servicios de valor agregado será necesario el consentimiento del titular de los datos personales.

Además, la geolocalización también puede tener implicaciones para la seguridad de la persona si no se protege adecuadamente la información sobre su ubicación. Saber dónde está en todo momento una persona puede ser utilizado para elaborar un perfil de sus actividades que podría llegar a ser utilizado con fines ilícitos. A través de la información derivada de la geolocalización podría ser posible saber dónde vive una persona, a qué hora sale y regresa a su casa, dónde trabaja o qué lugares de ocio visita.[88]

[87] El Grupo de Trabajo del artículo 29 indica que no obstante "hay muchos otros servicios que procesan datos de localización que también pueden plantear problemas de protección de datos y que van desde los sistemas de billetería electrónica hasta los sistemas de peaje para automóviles, o desde servicios de navegación por satélite hasta el seguimiento de la posición, por ejemplo con ayuda de cámaras, y la geolocalización de direcciones IP", p. 3.

[88] En el documento del Grupo de Trabajo del artículo 29, WP 185, se indica también que los servicios de geolocalización permiten "disponer de una panorámica detallada de los hábitos y pautas del propietario de estos dispositivos y establecer unos perfiles exhaustivos. A partir de un periodo de inactividad nocturna, puede deducirse el lugar donde duerme la persona, y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa. El perfil puede incluir, asimismo, datos derivados de las pautas de movimientos de sus amigos, sobre la base de lo que se conoce como "gráfica social", p. 7.

5. LA PROTECCIÓN DE DATOS PERSONALES EN INTERNET

En el caso de Internet, también como servicio de telecomunicaciones, se produce un tratamiento de datos personales que implica que se deba prestar atención a los diferentes aspectos o cuestiones que se plantean, tales como si la dirección IP es o no un dato personal, el uso de diferentes servicios como la navegación o el correo electrónico, así como las redes sociales y también otros aspectos como el "derecho al olvido" en Internet.

El usuario tiene que ser consciente de que al hacer uso de estos y otros servicios se produce o puede producir un tratamiento de sus datos personales, de manera que también tiene que hacer un uso responsable de la tecnología, por ejemplo revisando los controles de privacidad (en inglés, "privacy settings") de los productos o servicios, para ver si se ajustan a sus preferencias.

En relación con Internet y algunos servicios relacionados con el mismo, el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), proporciona información y consejos dirigidos a los usuarios con la finalidad de proteger su derecho fundamental a la protección de datos personales. Por ejemplo, a través de su cuenta de Twitter (@ InfoDF) el InfoDF proporciona consejos prácticos sobre protección de datos personales relativos a las redes sociales y también lleva a cabo otras importantes actividades, tales como trabajar con las autoridades capitalinas para crear un protocolo para combatir el acoso en redes sociales.

Por último, prestar atención a otras cuestiones de actualidad, como por ejemplo el "derecho al olvido", que permitiría a las personas que se borren sus datos personales una vez transcurrido cierto periodo de tiempo, puede ser relevante tanto para los usuarios de Internet como para otras partes interesadas dadas las implicaciones que puede tener en particular este derecho (resumen del capítulo elaborado por el autor del ensayo).

5.1. Internet como servicio de telecomunicaciones

El Internet[89] es uno de los servicios de telecomunicaciones que proporciona a los usuarios importantes beneficios sociales y económicos, ya que a través de Internet es posible acceder a multitud de servicios y aplicaciones, tales como el correo electrónico, las redes sociales, las páginas y sitios web, etc., de manera que se puede hacer uso del mismo como usuarios de dichos servicios y también como profesionistas que, por ejemplo, tienen páginas o sitios web de comercio electrónico,[90] etcétera.

Permite, también, la búsqueda y acceso de información, la comunicación con otras personas, juegos, etc., lo que implica que el Internet aporte importantes beneficios sociales. A modo de ejemplo en este sentido, cabe resaltar que según el Estudio sobre los Hábitos de los Usuarios de Internet en México 2015 de la AMIPCI, los principales usos de Internet son para acceder a redes sociales (85%), la búsqueda de información (78%), enviar y recibir correos electrónicos (73%), el uso de chats (enviar/recibir mensajes instantáneos, 64%) y la compra en línea (25%), seguido por otras actividades.

Al usar Internet es necesario saber que los datos personales del usuario son, o pueden ser, tratados

[89] Véase la definición dada en la fracción XXXII del artículo 3 de la LFTR.

[90] Según el Estudio de Comercio Electrónico en México 2015, de la Asociación Mexicana de Internet (AMIPCI), el comercio electrónico ha aumentado en México desde 2009 y que, con respecto a 2013, el comercio electrónico aumentó 34% en 2014, alcanzando una cifra de 162.10 billones de pesos, lo que supone 12.2 billones de dólares calculados conforme a un tipo de cambio promedio en 2014 de 13.28 pesos por un dólar. Dicho estudio está disponible en <https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf>.

por los diferentes sujetos que intervienen en cada caso. En este sentido, para poder acceder a Internet es necesario hacerlo a través de una conexión que es proporcionada por un concesionario. Este concesionario utiliza los datos personales del usuario para proporcionar y facturar, en su caso, el servicio.

No obstante, se puede acceder a Internet en un cibercafé o en un sitio público, de manera que habría que ver en cada caso de qué datos personales se tratan, por quién y para qué.

Otros agentes o figuras que podrían intervenir son los prestadores de servicios de Internet, siendo muchas las posibilidades ya que entre los mismos se encuentran quienes ofrecen servicios como el correo electrónico, los proveedores de contenidos como páginas y sitios web de información o comercio electrónico, así como otros servicios relativos a redes sociales, sitios de descargas, etc. Incluso puede ocurrir que en ocasiones el concesionario que proporciona acceso a Internet sea también un proveedor de servicios de Internet por tener su propia red social, servicio de correo electrónico, etcétera.[91]

En cualquier caso, al hacer uso de Internet y los servicios relacionados con el mismo, se produce un tratamiento de datos personales que deja una "huella digital" desde el momento mismo en que el usuario se conecta. Incluso se puede producir un tratamiento de datos personales que es "invisible" para el usuario[92] ya que, por ejemplo cuando se abre el navega-

[91] Una descripción de estos agentes que tratan datos personales en relación con Internet, así como algunas cuestiones relativas al funcionamiento de dicho servicio, pueden verse en Grupo de Trabajo del artículo 29, *Documento de trabajo. Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea*. En relación con el tratamiento de datos personales en Internet, en general, puede verse también el documento de este Grupo de Trabajo titulado *Documento de trabajo: tratamiento de datos personales en Internet*, WP 16, adoptado el 23 de febrero de 1999 y disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp16_es.pdf>.

[92] En relación con este tratamiento invisible, puede verse el documento del Grupo de Trabajo del artículo 29 titulado *Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware*, WP 17, aprobada el 23 de febrero de 1999 y disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp17_es.pdf>.

dor y se teclea la dirección de una página web, se produce un intercambio de información relativa al usuario, tales como la dirección IP, el idioma en el que está configurado el navegador u otra información que, concerniente a una persona física identificada o identificable, son datos personales.[93]

Este tratamiento de datos personales puede producirse también cuando se utilizan *cookies*,[94] esto es, archivos que se envían desde una página o sitio web para ser almacenados en el navegador del usuario y que pueden ser utilizados con diferentes fines; por ejemplo, autenticación del usuario, gestión del tráfico de usuarios de la página o sitio web, o también para identificar los gustos y preferencias del usuario. En este sentido, si se produce un tratamiento de datos personales a través del uso de *cookies*, dicho tratamiento tendrá que cumplir con la normatividad aplicable sobre protección de datos personales.

El tratamiento de datos personales que puede producirse en ciertos casos en Internet ha dado lugar, a nivel internacional, a que surjan también propuestas con la finalidad de garantizar la protección de datos y privacidad de los usuarios. Por ejemplo, una de estas propuestas es lo que se conoce como *Do Not Track*,[95] que puede traducirse como "no me

[93] Véase Grupo de Trabajo del artículo 29, *Documento de trabajo. Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea*. En concreto, en este documento se explica qué significa el "charloteo del navegador" que se produce cuando el usuario solicita, por ejemplo, ver una página web en su navegador. Dicho charloteo consiste, básicamente, en un intercambio de información necesaria para mostrar la página web en el navegador del usuario, pudiendo producirse un tratamiento de datos personales relativos al mismo, tales como su idioma o qué navegador tiene, entre otros.

[94] Definidas en la fracción I, del lineamiento tercero de los Lineamientos del Aviso de Privacidad, como "Archivo de datos que se almacena en el disco duro del equipo de cómputo o del dispositivo de comunicaciones electrónicas de un usuario al navegar en un sitio e Internet específico, el cual permite intercambiar información de estado entre dicho sitio y el navegador del usuario. La información de estado puede revelar medios de identificado de sesión, autenticación o preferencias del usuario, así como cualquier dato almacenado por el navegador respecto al sitio de internet."

[95] En concreto, la Comisión Federal de Comercio de Estados Unidos de América (en inglés, *Federal Trade Commission*, FTC) emitió algunas recomendaciones al respecto en 2010 en relación con la protección de los consumidores en línea (*online*). Dichas recomendaciones eran parte de un informe elaborado para promover la protección de la privacidad de los consumidores en línea. Puede verse más información al respecto en <http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track>. En el caso de la Unión Europea, el Grupo de Trabajo del artículo 29 emitió

rastrees", y que se planteó inicialmente para evitar el seguimiento de usuarios de Internet con fines de publicidad.

Al respecto, el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE ha indicado que:[96]

> La mayoría de las tecnologías de rastreo y publicidad utilizadas para producir publicidad comportamental recurren a algún tipo de tratamiento de datos del cliente. Utilizan información del buscador y del terminal del usuario. En especial, la principal tecnología de rastreo utilizada para controlar a los usuarios en internet se basa en "cookies de rastreo". Los cookies dan la posibilidad de rastrear las búsquedas del usuario a lo largo de un lapso extenso de tiempo y teóricamente en dominios diferentes."

El rastreo del usuario mediante estas *cookies*, utilizadas por los proveedores o distribuidores de redes de publicad o similares, tiene como fin poder saber qué publicidad le interesa al usuario que accede a una página web donde aparece un anuncio de la red de dicho distribuidor. De esta manera, el proveedor de la red de publicidad, a través de la *cookie* que le permitirá reconocer al usuario cuando vuelva a acceder a la página o sitio web en la que se incluye la publicidad de su red, podrá personalizar la publicidad de manera que la próxima vez que el usuario acceda vea anuncios o publicidad que pueda ser de su interés en virtud de la que ha visto durante las visitas anteriores.

La posibilidad de ver o recibir publicidad personalizada es un beneficio para muchas personas, pero requiere adoptar también medidas que permitan que aquellas otras que no quieren ver o recibir esta publicidad puedan hacerlo, además de que la publicidad implica el tratamiento de datos personales que tiene que cumplir con los principios y derechos aplicables.

---

su *Dictamen 2/2010 sobre publicidad comportamental en línea*, WP 171, adoptado el 22 de junio de 2010 y disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf>.

[96] Véase el documento WP 171, citado anteriormente, p. 6.

Es así que el mecanismo conocido como *Do Not Track*, consiste en que los usuarios tengan la posibilidad de oponerse a que, a través de una *cookie*, una página o sitio web que visitan, recabe información acerca de su navegación para ser usada con fines tales como presentarle publicidad personalizada.

Algunos proveedores de *software* y otras aplicaciones informáticas, como por ejemplo Microsoft, han desarrollado ya funcionalidades que ayudan a mantener privada la sesión de navegación, protegiendo así los datos del usuario. En concreto, y como ejemplo, Microsoft ha incluido en las últimas versiones de su navegador Internet Explorer la posibilidad de activar o desactivar la función *Do Not Track* a través de las opciones de seguridad del mismo.

Además de esta función, Microsoft ofrece también en su navegador la posibilidad de hacer una navegación sin dejar rastro de la sesión a través de *InPrivate*, que es también una función de las últimas versiones de Internet Explorer.[97] En este caso concreto, cuando el usuario se conecta a Internet a través de redes públicas o lo hace usando el equipo de otra persona o de un cibercafé, la posibilidad de hacer una exploración privada permite que, por defecto, no se almacene el historial de las páginas visitadas, los datos de formularios y contraseñas.

Es así que, al hacer uso de Internet y los diferentes servicios relacionados con el mismo, el usuario tiene que ser consciente de que se produce un tratamiento de sus datos personales, que puede usarse con diferentes finalidades y que, al respecto, puede y debe configurar, en su caso, los controles o parámetros de privacidad (en inglés, *privacy settings*) de las herramientas y servicios de los que haga uso en función de sus preferencias.

En el caso de niños y menores, los padres o tutores legales deben prestar especial atención al uso que éstos hagan de Internet y de determinados servicios, ya que la supervisión es importante para evitar riesgos a los menores, sin que dicha supervisión se convierta en una vigilancia para garantizar así también la libertad de los mismos.

[97] Sobre qué es la exploración *InPrivate* de Microsoft, puede verse más información en <http://windows.microsoft.com/es-es/windows/what-is-inprivate-browsing#1TC=windows-1>.

5.2. La dirección IP como dato personal o no

Una cuestión llamativa que dio lugar, hace ya años, a un intenso debate, especialmente entre representantes de la Unión Europea y de Estados Unidos, es la relativa a si una dirección IP es un dato personal o no.[98]

En cuanto a considerar que una dirección IP es un dato personal, el Grupo de Trabajo del artículo 29 ha indicado que:[99]

> [...] en la mayoría de los casos –incluso en casos con asignación de una dirección IP dinámica– estarán disponibles los datos necesarios para identificar al usuario o usuarios de la dirección IP.

Incluso el Grupo de Trabajo del artículo 29 se había pronunciado ya al respecto sobre las direcciones IP dinámicas indicando que:[100]

> Un caso particular sería el de algunos tipos de direcciones IP que en determinadas circunstancias y por diversas razones técnicas y organizativas no permiten realmente la identificación del usuario. Así sucede, por ejemplo, con las direcciones IP atribuidas a un ordenador instalado en un cibercafé, en el que no se pide identificación alguna a los clientes. En este caso, puede argüirse que los datos recogidos sobre el uso de un determinado ordenador "X" durante una determinada franja horaria, no permiten la identificación del usuario con medios razonables y, por lo tanto, no son datos

[98] Al respecto, véase a Aoie White (2008), *IP Addresses Are Personal Data, E.U. Regulator Says*, Washington Post, disponible en <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html>; Saul Hansell (2008), *I.P. Address: Partially Personal Information*, New York Times, disponible en <http://bits.blogs.nytimes.com/2008/02/24/ip-address-partially-personal-information/?_r=1#comment-113195>; y "Google, contrario a considerar las direcciones IP como un dato personal", *El País*, disponible en <http://tecnologia.elpais.com/tecnologia/2008/05/29/actualidad/1212049680_850215.html>.

[99] Véase Grupo de Trabajo del artículo 29 (2008), *Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda,* WP 148. Disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_es.pdf>, p. 9.

[100] Véase Grupo de Trabajo del artículo 29 (2007), *Dictamen 4/2007 sobre el concepto de datos personales, WP 136*. Disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf>, pp. 18-19.

personales. Sin embargo, cabe señalar que, muy probablemente, los prestatarios de servicios de Internet no sabrán si la dirección IP en cuestión permite la identificación o no, y tratarán los datos asociados a ese IP de la misma manera que tratarían la información asociada a las direcciones IP de los usuarios debidamente registrados e identificables. Así pues, a menos que el prestatario de servicios de Internet sepa con absoluta certeza que los datos corresponden a usuarios que no pueden ser identificados, tendrá que tratar toda información IP como datos personales, para guardarse las espaldas.

Que la dirección IP sea considerada como un dato personal o no tiene importantes consecuencias en la práctica, ya que si lo es, será necesario cumplir en su caso con la normatividad, tanto general como sectorial o específica, aplicable en materia de protección de datos personales. Por el contrario, de no ser considerada un dato personal, por no referirse a una persona física identificada o identificable, no habrá que aplicar dicha normatividad.

En cualquier caso, la evolución de Internet hacia el Internet de las Cosas (en inglés, *Internet of Things*, IoT), plantea también cuestiones relevantes por tener en consideración. En relación con el Internet de las Cosas, es necesario poner también el foco en el hecho de que cada vez hay más objetos conectados y que no siempre se trata de personas sino también de cosas, relacionadas en algunos casos con personas, como por ejemplo los autos, contadores u otros aparatos domésticos inteligentes (televisión, refrigerador, etc.), e incluso los vestibles (en inglés, *wearables*). Esto ya da lugar al conocido *big data*, que supone la obtención de ingentes cantidades de información, personal o no, procedente de diferentes fuentes lo que ocasiona, en algunos casos, que los datos se recaben sin que los usuarios se den cuenta de ello.

Concluir que una dirección IP es un dato personal o no depende de diversos aspectos que habrá que tomar en consideración en el análisis de cada caso concreto.[101] Si quien trata la dirección IP puede identificar

[101] Al respecto, puede verse el informe preparado para la Comisión Europea por Time.lex (2011), *Study of case law on the circumstances in which IP addresses are considered personal data, Final report*. Disponible, en inglés, en <http://www.timelex.eu/

a la persona a la que corresponde, entonces será un dato personal; si por el contrario no se refiere a una persona física o no es identificable,[102] entonces no será considerado como un dato personal, lo que excluye la aplicación de la normatividad en la materia.

Desde el punto de vista del usuario, que su dirección IP sea o no un dato personal tiene importancia, ya que debe ser consciente de que cuando se conecta a Internet o a un servicio electrónico utilizando su dispositivo, por ejemplo un celular inteligente, su dirección IP deja un rastro electrónico que permite saber dónde, a qué hora y, en su caso, a qué página o sitio web o qué servicio utilizó. Por lo tanto, es importante también que el usuario sepa que el tratamiento de sus datos personales, así como sus acciones en el entorno electrónico, tienen consecuencias.

5.3. Navegación

Uno de los principales usos relacionados con Internet es el relativo a la navegación o exploración haciendo uso de un navegador.

Según los datos incluidos en el *Estudio sobre los hábitos de los usuarios de internet en México 2015* de la AMIPCI, el tiempo promedio de conexión del internauta mexicano es de 6 horas y 11 minutos, lo que supone un aumento de 24 minutos con respecto al año anterior (2014), siendo el principal lugar de conexión el hogar, a través de una conexión WIFI,[103] los días viernes.

Cuando el usuario navega a través de páginas o sitios web, o utiliza el navegador como interfaz para acceder a diferentes servicios, tales como redes sociales, correo electrónico, etc., se produce un tratamiento de datos personales en los términos ya mencionados.

frontend/files/userfiles/files/publications/2011/IP_addresses_report_-_Final.pdf>.

102 En este sentido, es necesario recordar la definición del Reglamento de la LFPDPPP de persona física identificable: "Toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas."

103 Se trata de la conexión sin cable.

Por esta razón, el usuario tiene que ser consciente de que la navegación por Internet puede implicar un tratamiento de sus datos personales, pudiendo darse el caso de que quien trata estos datos esté situado fuera de México y es probable que no le sea aplicable la normatividad mexicana en materia de protección de datos personales. Es decir, cuando se hace uso de cualquier servicio, ya sea de correo electrónico, redes sociales, etc., relacionado con Internet, es importante que el usuario se informe a través del correspondiente aviso de privacidad, si lo hay, y de los términos y condiciones en materia de privacidad, en su caso, sobre quién, cómo y para qué se van a tratar sus datos personales.

Al respecto, también es importante poner atención en que algunos servicios electrónicos, tales como cuentas de correo electrónico, servicios de cómputo en la nube, etc., se ofrecen utilizando en ocasiones la etiqueta de "gratis", pero realmente no lo son porque quien las ofrece utiliza los datos personales para el envío de publicidad o, incluso, accede al contenido del correo electrónico para enviar también publicidad personalizada, lo que supone una intromisión ilegítima al derecho a la inviolabilidad de las comunicaciones.

Es por ello que el usuario de Internet y de servicios electrónicos relacionados con éste tiene que informarse de quién va a tratar sus datos personales y para qué los va a usar. Se trata así de saber si el proveedor del servicio correspondiente, cuando le sea aplicable la normatividad mexicana, actúa conforme a la misma o si, por el contrario, utiliza los datos personales del usuario sin su consentimiento, para, por ejemplo, desarrollar nuevos servicios basados en dicha información o, incluso, vender esta información a terceros.[104]

[104] Al respecto, puede verse un interesante documento publicado en la Unión Europea por el Supervisor Europeo de Protección de Datos (2014), *Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*. Disponible, en inglés, en <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competition_law_big_data_EN.pdf>. En dicho documento, el Supervisor Europeo de Protección de Datos indica, en la p. 8, que "´free´ online services are ´paid for´ using personal data which have been valued in total at over EUR 300 billion and have been forecast to treble by 2020", lo que puede traducirse al español como "los servicios en línea ´gratis´ se ´pagan por´ el uso de datos personales que han sido valorados en un total de más de 300 billones de euros y se prevé que esta cifra se triplique en 2020".

Con independencia de que el usuario sea consciente del tratamiento de sus datos personales cuando navega y de que los mismos no sean utilizados con fines que, en su caso, no han sido autorizados, explotando así el valor económico de sus datos personales, éste tiene que adoptar también algunas medidas para navegar de forma segura en el mundo electrónico, al igual que camina a diario de forma segura por la calle.

Es así que al hacer uso de Internet, hay algunos consejos básicos e importantes que deben ser tomados en consideración por parte de los usuarios. Al respecto, el InfoDF ha publicado, y tuitea habitualmente en su cuenta de Twitter (@InfoDF), algunos consejos para una navegación segura, tal y como se muestra en la siguiente imagen.

Con este tipo de acciones, el InfoDF busca concientizar también a los usuarios de Internet sobre la importancia de hacer un uso adecuado, responsable y seguro de la tecnología que está a su servicio, de manera que sus datos personales estén protegidos y, por lo tanto, lo estén también ellos como titulares de los datos personales correspondientes.

Además de estos consejos que brinda el InfoDF, es conveniente considerar también otros consejos que pueden ser importantes a la hora de proteger los datos personales en línea:

- Configurar el navegador de manera que los controles de protección de datos personales o privacidad sean los adecuados, según las preferencias del usuario;

- Cuando se accede a un servicio electrónico que requiere de autenticación (nombre de usuario y contraseña) no marcar, o desactivar si estuviera marcado, la opción "Recordar mis datos", "Seguir conectado" o similar, para evitar que otra persona no autorizada pueda conseguir acceder a la cuenta del usuario;

- Consultar el aviso de privacidad y, en su caso, la política de protección de datos o privacidad y, si todavía hubiera dudas, contactar al responsable de la página, sitio web o servicio de que se trate, con la finalidad de que la persona o departamento de datos personales, si es una página, sitio web o servicio electrónico en México, o el contacto para fines de protección de datos personales o privacidad en otro caso, aclare esas dudas que puedan tenerse en relación con el tratamiento de datos personales;

- No descargar *software* o aplicaciones cuyo origen se desconozca e instalarlas en la máquina o dispositivo, ya que ello podría causar también daños como consecuencia de que tengan un virus o que permitan el acceso a personas no autorizadas;

- No responder correos electrónicos cuyo origen se desconoce o en los que se piden datos de la cuenta del usuario (nombre de usuario y contraseña, u otros datos personales), por ejemplo, para restaurar los datos de la cuenta del banco o la cuenta de usuario de un medio de pago. Estos e-mails, enviados por terceros con la única finalidad de conseguir datos personales del usuario, se conocen como *phishing* y pueden dar lugar a un robo de información para la suplantación de identidad;

- En el caso de acceso a Internet por niños o menores, configurar las opciones del navegador, si cuenta con ellas, para evitar un uso inadecuado de Internet, lo que implica también que los menores estén demasiado tiempo conectados o que accedan a contenidos que pueden no ser apropiados para ellos.

Es decir, el usuario también es responsable de proteger sus datos personales ya que puede tomar decisiones importantes, por ejemplo, sobre qué productos o servicios utilizar y, en su caso, configurar el nivel de protección de datos personales o privacidad que considera adecuado, según sus preferencias.

5.4. Correo electrónico

El correo electrónico es un servicio que la mayoría de las personas tienen y del que hacen uso a diario por las posibilidades que ofrece tanto en la esfera personal como en la profesional.

Siendo un instrumento fundamental de comunicación, el correo electrónico implica un tratamiento de datos personales sin perjuicio de que el contenido del mismo esté también sujeto a la protección que confiere el secreto o la inviolabilidad de las comunicaciones.

Al enviar correos electrónicos[105] es importante considerar varias cuestiones específicas por las implicaciones que pueden tener para el derecho fundamental a la protección de datos personales. Así, por ejemplo, una primera cuestión por considerar es que cuando se copia a varias personas hay que asegurarse, primero, de que los destinatarios del mensaje de correo electrónico y, en su caso, los archivos adjuntos, son quienes deben recibirlo. Es decir, se trata de asegurarse de que no se envía a otras personas o destinatarios indebidos o no previstos, ya que ello supondría que personas no autorizadas o no previstas pudieran, en su caso, tener acceso a datos personales, con lo que ello conlleva para el principio de confidencialidad.

Y una segunda cuestión es que, en ocasiones, hay que hacer uso de la copia oculta (CCO) si por ejemplo se envía un correo electrónico a un grupo de personas y sus direcciones de correo electrónico o, al menos las direcciones de algunas de ellas, deben mantenerse ocultas para evitar infringir la confidencialidad de dichos datos y revelarlos a otras personas.

[105] Para una explicación técnica y fácil de entender sobre el servicio de correo electrónico, puede verse el documento del Grupo de Trabajo del artículo 29, *Directiva 95/46/CE sobre Privacidad en Internet, WP 37*, pp. 32-33.

Los programas de correo electrónico permiten también configurar algunos controles o parámetros de manera que se puede proteger mejor la privacidad del usuario. Esto implica que el usuario debe revisar, en su caso, la configuración de su programa cliente o del servicio electrónico que utilice para hacer uso del correo electrónico.

Además, el uso del correo electrónico requiere también tomar las medidas necesarias con el fin de proteger los datos personales. Por ejemplo, el envío de un correo electrónico que lleve adjunto un documento o una base de datos con datos personales, especialmente cuando éstos son sensibles tales como los relativos a la salud, no debería hacerse a menos que se hayan adoptado medidas de seguridad adecuadas como por ejemplo el uso de una contraseña robusta para acceder al documento o a la base de datos, o se haga utilizando una firma electrónica de manera que sólo el emisor y el destinatario autorizado pueda acceder al mismo.

5.5. Redes sociales

Las redes sociales,[106] ya sean utilizadas con fines personales por menores y adultos, o incluso con fines profesionales por estos últimos, son uno de los servicios electrónicos más utilizados a diario por millones de usuarios.

Las posibilidades de compartir información, mantener el contacto con familiares u otras personas o conocer a nuevas personas, hacen que las redes sociales sean una oportunidad que representa importantes beneficios sociales.

Y para que sean un beneficio, es necesario que los usuarios sean conscientes de que al acceder y hacer uso de una red social se produce un tratamiento de sus datos personales, al igual que cuando se suben o publican, por ejemplo, fotografías y se comparten datos personales relativos, entre otros, a nombre y apellidos, fecha de nacimiento, dirección postal, número de teléfono o dirección de correo electrónico.

[106] En su Dictamen 5/2009 sobre redes sociales en línea, WP 163, adoptado el 12 de junio de 2009, el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, en la Unión Europea, las define como "plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes", p. 5. Disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf>.

En este sentido, el usuario de redes sociales puede tomar en consideración algunos consejos que proporciona el InfoDF con el fin de proteger sus datos personales.

Al hacer uso de redes sociales hay que considerar también quién es el proveedor de la misma, si está establecido en México o si, por el contrario, está en otro país; cuál es el aviso de privacidad y, en su caso, si tiene una política de protección de datos y qué términos y condiciones son aplicables para poder utilizar la red social. Se trata de evitar "quedar atrapado" en la red debido a que, por ejemplo, una cuenta de usuario sólo pueda ser desactivada, pero los datos personales (nombre de usuario, fotografías, etc.) se mantengan para siempre en la red social sin ser cancelados de manera efectiva.

Además, saber con quién se comparte información, ya sean datos personales, incluidas fotografías, u otros contenidos como mensajes, es fundamental para proteger la privacidad, de manera que el usuario de una red social tiene que revisar el nivel de protección que ésta le confiere y, en su caso, configurar los controles parámetros de protección de datos o privacidad (conocidos en inglés como *privacy settings*) de manera que se pueda ejercer un control efectivo de qué y con quién se comparte información.

Al respecto, el InfoDF desempeña un importante papel en relación con la protección de datos personales y los menores en las redes sociales. En concreto, tal y como se mencionaba en un comunicado de prensa[107] publicado en 2014, el InfoDF estaba ya trabajando con las autoridades capitalinas para crear un protocolo con el fin de combatir el acoso en redes sociales.

Las redes sociales ofrecen a los usuarios importantes posibilidades de comunicación, entre otros beneficios, si bien es necesario hacer un uso responsable de las mismas, lo que conlleva que, especialmente en el caso de los menores, éstos reciban formación y, en su caso, ayuda para proteger su información personal.[108]

La protección de datos personales en las redes sociales es una cuestión que implica a todos, comenzando por el propio usuario, titular de los datos personales, así como a otras partes involucradas entre las que se encuentran los responsables de la propia red social y las autoridades competentes.

Si bien los jóvenes, quienes son "nativos digitales", y otros usuarios de las redes sociales, pueden conocer muy bien cómo utilizar la tecnología, es necesario que sean conscientes de cuándo facilitar o no sus datos personales, o las implicaciones de sus acciones en el entorno electrónico.

También es importante que el usuario de las redes sociales no realice acciones que puedan implicar el tratamiento de datos personales sin consentimiento de terceros, ya sea amigos, hijos u otras personas al, por ejemplo, subir fotografías en las que aparecen dichos terceros.

[107] Véase el comunicado de prensa del 15 de octubre de 2014. Disponible en <http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=2084&Itemid=217>.

[108] En relación con esta labor de concientización, puede verse también el comunicado de prensa del InfoDF del 22 de octubre de 2014, en el que se menciona al comisionado ciudadano, Luis Fernando Sánchez Nava, quien indicó que el "objetivo es crear una cultura y conciencia en los ciudadanos de protegerse para evitar actos como el acoso, secuestro, discriminación laboral, trata de personas o el bullying, que se han incrementado recientemente entre los jóvenes, principalmente entre los menores de edad". Disponible en <http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=2095&Itemid=217>.

Resulta, por lo tanto, muy relevante el papel del InfoDF y otras autoridades garantes, quienes dedican recursos a promocionar el derecho fundamental a la protección de datos personales, al mismo tiempo que, por ejemplo, en el caso del InfoDF, se busca proteger también a los niños y jóvenes capitalinos contra el acoso en redes sociales.

La importante labor que desempeña el InfoDF concientizando a los usuarios de redes sociales, requiere también que dichos usuarios tengan en consideración los consejos que se les brindan, como por ejemplo los mensajes que el InfoDF tuitea con frecuencia en relación con la protección de los datos personales, tanto propios como de terceros, en las redes sociales.

5.6. El "derecho al olvido" en Internet

El conocido como "derecho al olvido" en Internet ha sido, y es, una de las cuestiones que ha centrado la atención de multitud de autoridades y personas por las implicaciones que tiene[109] o que puede tener.

Este derecho consiste en la facultad de que una persona pueda dirigirse a un buscador o motor de búsqueda para pedir que cuando el criterio de búsqueda sea el nombre y apellidos de la misma, no aparezcan resultados basados en dicha búsqueda o, lo que es lo mismo, se excluyan de la lista de resultados (en inglés, *delisting*). Es decir, si preguntamos al motor de búsqueda utilizando como criterio un nombre y apellidos, los resultados de dicha búsqueda no deben incluir los vínculos o ligas relativas a esa persona, si ha ejercitado su derecho al olvido.

No se trata de un derecho absoluto, ya que cada solicitud que se haga al buscador será evaluada conforme a criterios específicos para determinar si procede, o no, suprimir de la lista de resultados aquéllos a los que se llegaría utilizando como criterio de búsqueda el nombre y apellidos de la persona.[110] En la actualidad, este derecho aplica a los buscadores o motores de búsqueda en la Unión Europea.

Se trata de una cuestión relevante, ya que este derecho al olvido tiene importantes implicaciones tanto en materia de protección de datos personales como en otros aspectos. En relación con este tema, el comisionado presidente del InfoDF, Mucio Israel Hernández Guerrero, indica que este derecho:

[109] Sobre este derecho, véase María Álvarez Caro, "Reflexiones sobre la sentencia del TJUE en el asunto "Mario Costeja" (C-131/12) sobre derecho al olvido", *Revista Española de Derecho Europeo*, núm. 51, 2014, pp. 165-187.

[110] Al respecto, Google designó a un Consejo Asesor que publicó un informe sobre el derecho al olvido, con fecha 6 de febrero de 2015. Disponible, en inglés, en <https://drive.google.com/a/google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1>.

> […] permitiría a las personas que sus datos personales se borren después de un periodo de tiempo determinado y operaría en las esferas penal, crediticia y en el uso de plataformas tecnológicas como el Internet.
>
> El derecho al olvido en el ámbito penal implicaría que tras ser sentenciadas y haber pagado la condena, las personas podrían demandar que sus datos personales se borren del expediente judicial para así garantizar su reinserción social y la recuperación de su honor y de su fama pública.
>
> El comisionado ciudadano del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), puntualizó que este derecho no operaría en delitos de alto impacto como los de carácter sexual, la pederastia o la trata de personas.
>
> El derecho al olvido en el aspecto financiero garantizaría que quienes estén reportados en el Buró de Crédito por algún mal comportamiento financiero, puedan ser eliminados de ese listado en el momento en que cumplan sus obligaciones.[111]

Y también en el mismo comunicado de prensa, referido a las redes sociales, se indicaba que el derecho al olvido "significaría que las personas pudieran eliminar su 'rastro electrónico' cada seis meses".

> La sentencia del TJUE sobre el "derecho al olvido" en Internet
>
> El 13 de mayo de 2014 el Tribunal de Justicia de la Unión Europea (TJUE) dio respuesta a la cuestión prejudicial planteada por la Audiencia Nacional española a través de su sentencia sobre "el derecho al olvido".[112] En total, el TJUE daba respuesta a las nueve

[111] Véase el comunicado de prensa del 25 de marzo de 2013. Disponible en <http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=1522&Itemid=217>.

[112] Sentencia del Tribunal de Justicia (Gran Sala) del 13 de mayo de 2014, "Datos personales – Protección de las personas físicas en lo que respecta al tratamiento de dichos

preguntas[113] que se le habían planteado por la Audiencia Nacional española.

En este caso, una persona ejercitó ante un periódico, publicado por "La Vanguardia Ediciones, S.L." y de gran difusión especialmente en Cataluña, su derecho de oposición al tratamiento de sus datos personales ya que al introducir su nombre y apellidos en el buscador de Google, en los resultados de búsqueda aparecía una liga a una página del periódico donde había una referencia a una subasta de un bien raíz por un embargo debido a una deuda con la Seguridad Social. Según el afectado, el embargo ya había sido solucionado hace años y esta información carecía de relevancia actualmente.

El periódico respondió que su solicitud de cancelación de sus datos no procedía ya que la publicación se había hecho mediante una orden del Ministerio de Trabajo y Asuntos Sociales. Dicha respuesta fue confirmada por la Agencia Española de Protección de Datos (AEPD).

Pero el afectado también se dirigió a Google Spain, S.L., solicitando su derecho de oposición. Y en este caso sí procedía el derecho de oposición, por lo que la AEPD inició un procedimiento de tutela de derechos contra Google Spain, S.L. y Google Inc. Ante la resolución del Director de la AEPD, de fecha 30 de julio de 2010, Google Spain S.L. y Google Inc. recurrieron ante la Audiencia Nacional, que planteó una cuestión prejudicial al TJUE sobre la interpretación de la Directiva 95/46/CE sobre protección de datos en este caso.

datos – Directiva 95/46/CE – Artículos 2, 4, 12 y 14 – Ámbito de aplicación material y territorial – Motores de búsqueda en Internet – Tratamiento de datos contenidos en sitios de Internet – Búsqueda, indexación y almacenamiento de estos datos – Responsabilidad del gestor del motor de búsqueda – Establecimiento en territorio de un Estado miembro – Alcance de las obligaciones de dicho gestor y de los derechos del interesado – Carta de los Derechos Fundamentales de la Unión Europea – Artículos 7 y 8", en el asunto C-131/12. Disponible en <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=531281>.

[113] Estas preguntas pueden verse en el Auto de la Audiencia Nacional. Disponible en <http://www.poderjudicial.es/stfls/PODERJUDICIAL/JURISPRUDENCIA/FICHERO/20120227%20Auto%20ANCA%20REC%20725.2010.pdf>.

> Entre las cuestiones planteadas estaba la relativa a si: ¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?

A esta pregunta, el TJUE respondió lo siguiente:

> […] se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados, obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.
>
> (Resumen del caso elaborado por el autor del ensayo y citas de la sentencia del TJUE en el caso C-131/12.)

El derecho al olvido, como indicó durante la Semana Nacional de Transparencia 2014 el comisionado presidente del InfoDF, Mucio Israel Hernández Guerrero,[114] no es un derecho absoluto, como tampoco lo es el derecho fundamental a la protección de datos personales. Es así que este derecho al olvido, como indica Hernández Guerrero, encuentra sus límites en los derechos a la libertad de expresión e imprenta, así como en las fuentes originales, tanto periodísticas como históricas.

Asimismo, Hernández Guerrero afirma que "se diferencia de los derechos ARCO y particularmente de cancelación y oposición". Además, en ocasiones, su aplicación en la práctica no es tarea sencilla por las importantes implicaciones que tiene, como por ejemplo determinar, sin lugar a dudas, cuándo una información ya no es de interés público o su aplicación territorial.[115]

Las cuestiones que plantea el derecho al olvido, que pueden y deben ser analizadas desde diferentes perspectivas, tales como la jurídica, económica, social e incluso histórica, perdurarán en el tiempo. No obstante, por el momento, el Grupo de Trabajo del artículo 29 ha publicado unas directrices sobre la aplicación de la Sentencia del TJUE[116] en las que

[114] Su presentación, en el panel sobre "Sistemas, niveles de seguridad y vigilancia de los sistemas de datos personales" puede verse en <http://snt.ifai.org.mx/files/mtr_mucio_hdz.pptx>.

[115] En este sentido, véase European Union Agency for Network and Information Security –ENISA- (2012), *The right to be forgotten – between expectations and practice*. Disponible, en inglés, en <https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport>. Entre las principales recomendaciones hechas por ENISA en su informe, se encuentran las relativas a la necesidad de que legisladores y autoridades de protección de datos trabajen juntas para "clarificar las definiciones y facilitar la aplicación del derecho (aclaración sobre quién puede solicitar la supresión de datos personales compartidos, en qué circunstancias, etc.)". También considerar los costos asociados al ejercicio de este derecho, que "una solución puramente técnica para hacer respetar este derecho en la Internet abierta es imposible", o que es necesario considerar la aplicación de este derecho dentro y fuera de la Unión Europea. Véase el comunicado de prensa sobre el informe, del 20 de noviembre de 2012, disponible en <http://www.enisa.europa.eu/media/press-releases/nuevo-informe-de-la-agencia-europea-enisa-sobre-los-aspectos-tecnicos-del-derecho-a-ser-olvidado>.

[116] Grupo de Trabajo del artículo 29 (2014), *Guidelines on the implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc. v. Agencia*

interpreta algunos aspectos de dicha sentencia, y proporciona también una lista de criterios para que las autoridades europeas de protección de datos puedan gestionar las quejas que reciben.[117]

En relación con el derecho al olvido en México se han planteado dos casos relevantes ante el INAI. El primero de ellos se dio cuando la Junta Federal de Conciliación y Arbitraje (JFCA), que había resuelto un procedimiento laboral en 2004, solicitó a Google, en 2009 y como consecuencia de la reclamación presentada por el titular de los datos, que evitase "indexar", dejando de incorporarlo a la base de datos de sus motores de búsqueda, el nombre del recurrente en el procedimiento laboral señalado.[118] En este caso, el INAI confirmó las acciones que la JFCA había adoptado y que consistían, básicamente, en haber modificado el formato de los archivos bajo los cuales se publicaban los Boletines Laborales para que los motores de búsqueda no pudieran localizar e indexar el nombre del titular de los datos y pedir a Google que eliminara de sus índices la referencia del nombre del recurrente hacia los archivos en el formato original.

El segundo caso se planteó a finales de 2014 cuando una persona presentó una solicitud de protección de derechos ante el INAI ya que se mostró inconforme con la respuesta dada por Google México, S. de R. L. de C. V. en relación con su solicitud de ejercicio de derechos de cance-

Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, WP 225. Disponible, en inglés, en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>.

117 Cabe señalar que el Grupo de Trabajo del artículo 29 mantuvo en su momento reuniones con los principales motores de búsqueda en relación con el derecho al olvido, tal y como manifestó a través de un comunicado de prensa publicado con fecha 25 de julio de 2014 en el que incluía las preguntas hechas a los gestores de los motores de búsqueda que participaron en la reunión. El comunicado de prensa, en inglés, está disponible en <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140725_wp29_press_release_right_to_be_forgotten.pdf>.

118 Resolución del 16 de marzo de 2011, en el recurso de revisión con número de expediente 4198/09. Disponible en <http://consultas.ifai.org.mx/descargar.php?r=./pdf/resoluciones/2009/&a=4198.pdf>. También puede verse la nota Informativa que en su momento publicó el IFAI, hoy INAI. Disponible en <http://inicio.ifai.org.mx/pdf/resoluciones/2009/4198_Resumen.pdf>.

lación y oposición.[119] En concreto, el titular de los datos solicitaba que Google cancelase, suprimiese y bloquease ciertos resultados que aparecían en el buscador si se buscaba a través de su nombre. Ante la respuesta dada por Google, negando el ejercicio de los derechos de cancelación y oposición y absteniéndose de cancelar y dejar de tratar los datos personales del titular,[120] el INAI resolvió revocar la respuesta dada.

La resolución del INAI dio lugar a un amplio debate sobre el derecho al olvido que sirvió para poner de manifiesto la complejidad de esta cuestión y la necesidad de tener en consideración todos los aspectos que se plantean en relación con dicho derecho.

En particular, el derecho al olvido requiere delimitar claramente su alcance, lo que implica establecer, en su caso, criterios claros para ponderar los diferentes derechos que pueden estar en presencia en cada caso cuando alguien pide que se evite indexar los resultados basados en una búsqueda cuyos criterios son el nombre y apellidos de dicha persona. Al mismo tiempo, se debe considerar específicamente cómo implementar en la práctica este derecho, considerando a todas las partes interesadas y las implicaciones para las mismas.

[119] Resolución en el Expediente PPD.0094/14, relativo a la solicitud de protección de derechos y que revoca la respuesta dada por el responsable del tratamiento. Votada el 26 de enero de 2015. Disponible en <http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf>.

[120] Resolución en el Expediente PPD.0094/14, considerando Quinto, p. 31.

6. ALGUNAS REFLEXIONES FINALES

Los servicios de telecomunicaciones y en particular Internet, brindan a los usuarios la oportunidad de acceder a información y otros servicios, como por ejemplo, correo electrónico, redes sociales, banca electrónica, comercio electrónico, etc., que requieren que tanto los concesionarios de telecomunicaciones o autorizados como quienes prestan dichos servicios tengan que cumplir con la normatividad general y sectorial o específica en materia de protección de datos personales y privacidad. Al mismo tiempo, el usuario de dichos servicios tiene que saber que:

- La Constitución Política de los Estados Unidos Mexicanos incluye tanto el derecho fundamental a la protección de datos personales de los usuarios de telecomunicaciones e Internet, así como otros derechos relativos al secreto o inviolabilidad de las comunicaciones y al acceso a las tecnologías de la información y comunicación, incluyendo la banda ancha e Internet;

- El usuario de servicios de telecomunicaciones e Internet tiene derecho a que todo tratamiento de sus datos personales que se lleve a cabo, en los términos previstos en la ley, cumpla con la Ley Federal de Protección de Datos Personales

en Posesión de los Particulares (LFPDPPP) y demás normatividad aplicable, tanto general como sectorial o específica;

- Lo anterior implica que los concesionarios de telecomunicaciones o autorizados, que prestan o pueden prestar diversos servicios de telecomunicaciones e Internet, tienen que cumplir con dicha normatividad, garantizando así los derechos fundamentales de los usuarios;

- Cumplir con la normatividad sobre protección de datos personales y facilitar el uso de tecnología que ayude a proteger los datos personales, ayuda también a generar o, en su caso, impulsar la confianza de los usuarios con lo que ello supone para la innovación tecnológica;

- Es necesario que el usuario también se informe de quién, cómo y para qué se tratarán sus datos personales en el ámbito de los servicios de telecomunicaciones e Internet;

- Hay que considerar que, especialmente en Internet, pueden producirse tratamientos de datos que resultan desconocidos o son "invisibles" para los usuarios, de manera que es importante que el usuario conozca también cómo funcionan dichos servicios en cuanto al tratamiento de sus datos personales;

- El usuario también tiene obligaciones, debiendo hacer un uso responsable de la tecnología y de los diferentes servicios electrónicos. Por ejemplo, el usuario, como aconseja el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), no debe proporcionar o compartir sus datos personales en redes sociales con otros usuarios a los que no conoce, y debe revisar también los controles o parámetros de privacidad (en inglés, *privacy settings*) de los servicios que utiliza para asegurarse de que responden a sus preferencias;

- Cuando se le ofrece un servicio que se etiqueta como "gratuito", debe leer los términos y condiciones del mismo, específicamente en cuanto al tratamiento y uso de sus datos personales, ya que el

pago por dichos servicios podría consistir precisamente en el uso de sus datos personales;

- El InfoDF y otras autoridades garantes en protección de datos personales realizan acciones con el fin de ayudar a los usuarios a conocer sus derechos, cómo hacer un uso responsable de los servicios de telecomunicaciones e Internet, así como otras acciones dirigidas a proteger a los menores;

- En definitiva, los servicios de telecomunicaciones, incluyendo Internet, son una necesidad en todas las áreas o facetas de los usuarios, ya sea como consumidores o ciudadanos, de manera que el cumplimiento de la protección de datos personales y otros derechos fundamentales son una garantía para su uso y el desarrollo, tanto de una Sociedad de la Información y del Conocimiento como de una industria de servicios competitivos a nivel nacional e internacional.

Sin perjuicio de lo anterior, cabe señalar que en México se ha producido una evolución de la legislación en materia de protección de datos personales durante los últimos años y que se corresponden también con el auge de los servicios de telecomunicaciones y comunicaciones electrónicas, así como de la economía digital. Desde la publicación de la LFPDPPP, pasando por la reforma de las telecomunicaciones y hasta la Carta de Derechos Mínimos de los Usuarios de los Servicios Públicos de Telecomunicaciones, son pasos necesarios en el desarrollo de un marco adecuado para establecer un alto nivel de protección de los datos personales, garantizando así los derechos fundamentales a la protección de esos datos y a la privacidad.

No obstante, es necesario pensar en la necesidad de normas flexibles, en el sentido de que puedan ser adaptadas a los requerimientos de la sociedad en cada momento de la sociedad en cuanto a la protección de sus datos personales y privacidad. Dichas normas deben ser, por otro lado, robustas, en cuanto a la inclusión de principios, deberes y derechos aplicables de cara al futuro, evitando así el riesgo de una rápida obsolescencia que puede dar lugar a una protección ineficiente e ineficaz, así como crear obstáculos a la innovación que redunda en beneficio de la sociedad y de la economía.

Es por ello que resulta necesario alinearse con altos estándares internacionales, debiendo considerar en este sentido, por ejemplo, tanto instrumentos como el Convenio 108 del Consejo de Europa[121] como estándares entre los que cabe citar la ISO/IEC 27018 sobre privacidad en la nube,[122] que es el primer estándar internacional en la materia, y que ayudará a todas las partes, clientes de servicios de nube pública, proveedores de servicios de nube pública, así como a autoridades garantes y reguladoras, a alcanzar un alto nivel de protección de datos personales.

Esto implica también la necesidad de cooperación entre todas las partes interesadas, impulsando la cooperación público-privada en todos los ámbitos, ya que, por ejemplo, una suplantación de identidad puede requerir una respuesta en varios frentes, tanto en materia de protección de datos personales, como en la protección al propio consumidor, todo ello sin olvidar las consecuencias civiles o penales que pudiera tener el caso. Es decir, cada vez más se requieren acciones y respuestas comprehensivas, tanto a nivel nacional como internacional, que requieran de un alto nivel de compromiso por todas las partes involucradas.

La economía digital, basada en el uso de las telecomunicaciones e Internet, es una oportunidad que México no puede dejar pasar. Dicha economía gira en torno a los datos que, cuando son personales, requieren que quienes los tratan lo hagan con responsabilidad (en inglés, *accountability*), debiendo considerar que el objetivo de la normatividad y la autorregulación es proteger al titular de los datos personales, coadyuvando a generar confianza, al mismo tiempo que se busca también facilitar la innovación y la competitividad. La protección de datos personales y la privacidad son garantías que deben ser aplicadas con proporcionalidad, de

[121] Convenio 108 del Consejo de Europa del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible en <http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf>.

[122] Norma ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (puede traducirse al español como ISO/IEC 27018:2014 Tecnología de la información – Técnicas de seguridad – Código de práctica para la protección de la información personal identificable (IPI) en nubes públicas actuando como encargados del tratamiento de IPI. Sobre lo mismo, puede verse más información en <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498>.

manera que den lugar a barreras comerciales que privarían a los propios titulares de los datos personales de importantes beneficios.

El futuro que nos depara todavía el tratamiento de datos masivos (en inglés, *big data*), las aplicaciones (en inglés, *apps*), los vestibles (en inglés, *wearables*), así como los servicios de telecomunicaciones e Internet, requiere de sólidos cimientos en materia de protección de datos personales, debiendo considerar también la necesidad de evaluar qué normas son realmente necesarias, cuáles están obsoletas o requieren ser revisadas, por diferentes razones, así como el papel de la autorregulación. Y también la anonimización o disociación puede, cuando resulte aplicable, ser una estrategia que ayude a conseguir este objetivo de un alto nivel de protección de datos personales, sin perder importantes beneficios en cuanto a la posibilidad de hacer uso de datos abiertos.

En definitiva, considerar en qué casos específicos hay que tratar datos personales ayudará a generar confianza y garantizar el derecho fundamental a la protección de datos personales y a la privacidad. Considerar también excepciones a la aplicación de la normatividad sobre protección de datos personales, ya que no es un derecho absoluto, así como establecer criterios claros de qué es un dato personal, e impulsar en cualquier caso la autorregulación, es necesario para establecer un marco adecuado de condiciones para el desarrollo de servicios innovadores y competitivos, al mismo tiempo que se garantizan los derechos fundamentales a la protección de datos personales y a la privacidad, sin olvidar otros derechos fundamentales como, por ejemplo, el secreto de las comunicaciones y el acceso de banda ancha a Internet.

Recomendaciones básicas para las partes interesadas

La protección de datos personales en el ámbito de las telecomunicaciones e Internet es una cuestión que implica a todas las partes interesadas, entre las que se encuentran los usuarios de estos servicios, los proveedores de dichos servicios y las autoridades garantes en materia de protección de datos personales.

Es así que garantizar un alto nivel de protección de datos personales y privacidad requiere de acciones y la colaboración, en su caso, entre las diferentes partes implicadas, de manera que se impulse la confianza necesaria en el uso de la tecnología, que está al servicio del usuario proporcionando importantes beneficios sociales y económicos. Al mismo tiempo, se debe impulsar la innovación tecnológica, por lo que se refiere a los servicios de telecomunicaciones, la tecnología o los servicios electrónicos que tengan por objeto facilitar a los usuarios medidas para proteger sus datos personales y privacidad.

Esta confianza permitirá, también, el desarrollo de una industria tecnológica y la prestación de servicios electrónicos competitivos, tanto a nivel nacional como internacional, de manera que el diseño e implementación de planes u otras acciones basadas en considerar los derechos de los usuarios, en particular la protección de sus datos personales y privacidad, son claves y necesarias.

Es por ello que a continuación se incluyen algunas recomendaciones básicas que, en su caso, puedan servir a las diferentes partes interesadas en el desarrollo de sus planes o acciones para promover y garantizar la protección de datos personales en el ámbito de las telecomunicaciones e Internet.

Recomendaciones dirigidas a los usuarios de servicios de telecomunicaciones e Internet

1. *El usuario es titular de derechos y entre ellos el derecho fundamental a la protección de datos personales.* El usuario de servicios de telecomunicaciones e Internet es titular de derechos, como el derecho fundamental a la protección de sus datos personales, y otros derechos como el relativo al secreto o inviolabilidad de las comunicaciones y el acceso a las tecnologías de la información, de manera que debe ejercerlos de forma responsable, conociendo su significado y alcance;
2. *Los menores son también titulares del derecho fundamental a la protección de datos personales.* Los menores son también titulares de sus datos personales, debiendo tener en consideración los casos en los que pueden ejercer por sí mismos su derecho fundamental a la protección de datos personales o aquellos otros en los que dicho ejercicio se hará a través de sus padres o tutores legales;
3. *El usuario de servicios de telecomunicaciones e Internet tiene obligaciones.* El usuario también tiene obligaciones, de manera que debe informarse sobre el tratamiento y uso de sus datos personales así como, en su caso, requerir información a quien trata o va a tratar sus datos personales sobre el uso de los mismos;
4. *El usuario debe revisar los controles o parámetros de privacidad.* Es importante que el usuario revise los controles o parámetros de privacidad (en inglés, *privacy settings*) de los productos o servicios que utiliza con la finalidad de establecer un nivel de protección de datos personales o privacidad adecuado, según sus preferencias;
5. *El usuario debe cuidar también que sus datos personales no sean utilizados como moneda de pago por los servicios que utiliza.* Hay una multitud de servicios de telecomunicaciones y electrónicos, que pueden ser gratuitos, disponibles para los usuarios y sobre los que éstos tienen que informarse antes de hacer uso de los mismos, por lo que se refiere al tratamiento o uso de sus datos personales, para evitar así que éstos puedan convertirse en la "moneda de pago";

6. *El usuario debe informarse y hacer un uso responsable de los servicios y la tecnología.* Es importante que el usuario se informe sobre cómo hacer un uso responsable, seguro y adecuado de la tecnología para obtener así los máximos beneficios posibles. Además, el usuario debe ser consciente de que aunque no lo vea directamente, puede producirse un tratamiento de sus datos personales al usar determinados servicios, y debe evitar proporcionar más datos personales de los que son necesarios para tal fin;
7. *El usuario debe proteger sus datos personales y privacidad.* El usuario debe adoptar medidas para proteger sus datos personales y privacidad, por ejemplo, no compartiendo información con desconocidos en redes sociales o respondiendo a correos electrónicos cuyo origen es desconocido y que podrían tener como finalidad conseguir su información personal para suplantar su identidad (conocido en inglés, como *phishing*);
8. *El usuario debe consultar e informarse en materia de protección de datos personales.* El usuario tiene a su disposición información que puede ser proporcionada por diferentes partes, tales como las autoridades garantes, de manera que puede, y debe, hacer uso de la misma para conocer las implicaciones que puede tener el uso de los servicios de telecomunicaciones e Internet para su derecho fundamental a la protección de datos personales;
9. *El usuario puede pedir ayuda a las autoridades garantes y, entre ellas, al InfoDF.* Cuando surgen dudas o problemas, además de dirigirse a quien le proporciona el servicio correspondiente, el usuario también puede acudir a las autoridades garantes, entre las que se encuentra el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF) en el caso de quienes viven en el Distrito Federal;
10. *El usuario, como titular del derecho fundamental a la protección de datos personales, debe conocer su significado y alcance.* En definitiva, el usuario, como titular de sus datos personales, tiene que conocer y valorar el significado de su derecho fundamental a la protección de datos personales, de manera que es quien tiene el control sobre el tratamiento de sus datos personales, pudiendo ejercer para tal fin los derechos que la ley, a través de la normatividad general y sectorial o específica, le reconoce.

Recomendaciones dirigidas a los proveedores de servicios de telecomunicaciones e Internet

1. *Los concesionarios de telecomunicaciones y proveedores de servicios tienen que adoptar medidas para cumplir con la normatividad aplicable en materia de protección de datos personales.* Los concesionarios de telecomunicaciones o autorizados y demás proveedores de servicios (en lo sucesivo, proveedores de servicios) que están sujetos a la normatividad en materia de telecomunicaciones, tienen que cumplir además con la normatividad sobre protección de datos personales, adoptando las medidas necesarias para garantizar el derecho fundamental a la protección de datos personales de sus usuarios o potenciales usuarios;
2. *Los proveedores tienen que ser transparentes en los términos y condiciones de sus servicios, especialmente por lo que se refiere al tratamiento de datos personales.* Es importante que estos proveedores proporcionen toda la información necesaria, especialmente en materia de tratamiento de datos personales, a sus usuarios y potenciales usuarios, para que así éstos puedan tomar decisiones informadas sabiendo claramente con qué fin se van a tratar sus datos personales. Además, los proveedores tienen que cumplir también con los principios que legitiman, en cada caso, dicho tratamiento de datos personales, los deberes de seguridad y confidencialidad, y adoptar medidas para atender el ejercicio de derechos de acceso, rectificación, cancelación y oposición;
3. *Los proveedores tienen que proporcionar información completa y fácil de comprender.* En particular, por lo que se refiere al tratamiento de datos personales, los proveedores tienen que proporcionar la información necesaria, de manera sencilla y que esté expresada en un lenguaje claro y comprensible. Se trata así de que cualquier usuario pueda comprender, sin necesidad de conocimientos específicos, qué datos personales y para qué fin se van a tratar, además de otros términos y condiciones del servicio del que hace uso. Es también importante que esta información sea completa y no requiera que el usuario tenga que remitirse a otros lugares o medios para conseguirla;

4. *Los proveedores tienen que tratar los datos personales de acuerdo con altos est*ándares nacionales e internacionales *en la materia.* Los proveedores de servicios tienen que desarrollar productos o servicios y, en su caso, prestarlos conforme a la normatividad aplicable y altos estándares, nacionales e internacionales, en materia de protección de datos personales, privacidad y seguridad. Se trata así tanto de proteger al titular de los datos personales como de proporcionar productos o servicios que sean competitivos al garantizar un alto nivel de protección de datos personales;
5. *Cuando utilizan los datos personales para fines de publicidad, los proveedores tienen que hacerlo conforme a la normatividad aplicable.* De manera que no se vulnere el derecho fundamental a la protección de datos personales, lo que implica, en concreto, que tengan que obtener el consentimiento necesario para tal fin además de, en su caso, no realizar ningún tratamiento que pueda vulnerar otros derechos fundamentales al secreto o inviolabilidad de las comunicaciones, tales como acceder al contenido de correos electrónicos u otras comunicaciones para hacer uso del mismo con fines publicitarios;
6. *Los proveedores deben considerar en particular la minimización del tratamiento de los datos personales.* De manera que traten sólo aquellos datos personales que son estrictamente necesarios en cada caso, lo que además ayuda a cumplir con principios esenciales, como por ejemplo el relativo a la calidad de los datos personales. Además, al minimizar los datos personales se facilita el cumplimiento de otros principios, como el de finalidad, y se evita que éstos sean tratados por más tiempo del necesario o para otras finalidades diferentes y, por lo tanto, incompatibles con aquellas para las que los datos fueron obtenidos;
7. *Los proveedores deben considerar la adopción de medidas de autorregulación.* La autorregulación en protección de datos personales, y en otras áreas, puede ayudar a aumentar el nivel de protección de datos personales, de manera que los proveedores deben considerar el desarrollo o, en su caso, la adopción de medidas de autorregulación tales como códigos de conducta, códigos éticos o certificaciones que les sirvan para alcanzar un alto nivel de protección de datos personales en la prestación de

sus servicios o el desarrollo de productos relacionados con las tecnologías de la información;

8. *Los proveedores tienen que adoptar medidas para asegurar la confidencialidad y seguridad de los datos personales que tratan.* En virtud de la normatividad general y sectorial o específica aplicable, los proveedores de servicios de telecomunicaciones e Internet tienen que adoptar también medidas para garantizar la confidencialidad en el tratamiento de los datos personales; en su caso, el secreto o inviolabilidad de las telecomunicaciones o los servicios relacionados con Internet que proporcionan, así como la seguridad administrativa, física y técnica;
9. *Los proveedores deben colaborar con las autoridades garantes en fomentar y garantizar la protección de datos personales.* Los proveedores deben considerar la necesidad e importancia de colaborar con autoridades garantes, tales como el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), con la finalidad de llevar a cabo acciones o adoptar medidas que permitan proteger, de manera efectiva, al titular de los datos personales, al mismo tiempo que se siga desarrollando una cultura de protección de datos personales en la que participen todas las partes interesadas e involucradas en la defensa y promoción del derecho fundamental a la protección de datos personales;
10. *Los proveedores tienen que adoptar medidas para generar, fomentar y mantener la confianza necesaria.* Los proveedores son una de las partes interesadas fundamentales, ya que son quienes proporcionan servicios y, en su caso, desarrollan o facilitan productos o servicios tecnológicos. Por lo tanto, son una pieza clave en lo que se refiere a generar y, en su caso, mantener la confianza necesaria de los usuarios, debiendo colaborar para tal fin tanto con las autoridades garantes y otras autoridades competentes como con los usuarios, a través de medidas como la evaluación del impacto de privacidad, el desarrollo de productos o servicios partiendo de la privacidad desde el diseño u otras medidas que puedan adoptar en virtud del principio de responsabilidad o rendición de cuentas (en inglés, *accountability*).

Recomendaciones dirigidas a las autoridades garantes

1. *Las autoridades garantes de protección de datos personales son clave para proteger al titular de los datos personales.* Ya que en el ejercicio de las competencias y facultades que tienen atribuidas las autoridades garantes de protección de datos personales, entre las que se encuentra el InfoDF, se logra que quienes proporcionan servicios de telecomunicaciones e Internet cumplan con sus obligaciones y, por lo tanto, se respete el derecho fundamental a la protección de datos personales de los usuarios de dichos servicios, como titulares de los datos personales que se tratan. Además, estas autoridades garantes cumplen otras importantes funciones en relación con el desarrollo de una cultura de protección de datos personales;
2. *Las autoridades garantes tienen que conocer las implicaciones de la tecnología para la protección de datos personales y viceversa.* De no ser así, se podría producir una situación en la que se obstaculice la innovación tecnológica y no se proteja de manera adecuada y efectiva el derecho fundamental a la protección de datos personales. Por lo tanto, es importante que las autoridades garantes analicen y conozcan qué implicaciones tienen los servicios de telecomunicaciones e Internet para el derecho fundamental a la protección de datos y otros derechos fundamentales por considerar en la búsqueda de un equilibrio necesario;
3. *Las autoridades garantes deben considerar también aspectos internacionales.* Especialmente en el ámbito del tratamiento de datos personales en las telecomunicaciones e Internet, ya que la tecnología y los servicios electrónicos van más allá de las fronteras nacionales, lo que supone, entre otras cuestiones, que los usuarios puedan acceder a servicios que son prestados por proveedores establecidos en otros países, o también que se publiquen datos personales en redes sociales, páginas o sitios web que quedan fuera de la jurisdicción de la autoridad garante por lo que, en su caso, puede ser necesaria la cooperación internacional con otras autoridades de protección de datos personales;

4. *Las autoridades garantes deben promover la adopción de esquemas de autorregulación en protección de datos.* Con la finalidad de alcanzar un alto nivel de protección de datos personales, las autoridades garantes deben promover la adopción de esquemas de autorregulación vinculante en protección de datos personales, incluyendo la certificación. La autorregulación es un instrumento adecuado para tratar cuestiones específicas relativas a un sector concreto de actividad, como por ejemplo las telecomunicaciones, por lo que promover el desarrollo o, en su caso, adopción de la misma, es una opción a considerar;
5. *Las autoridades garantes tienen que proteger a los titulares de los datos personales y también proporcionarles información.* Se trata de que las autoridades de protección de datos protejan a los titulares de los datos personales en el ejercicio de sus derechos (ARCO), velen o vigilen por el cumplimiento de los principios y deberes exigibles a quienes tratan sus datos personales, y también les proporcionen a los usuarios información sobre el significado de su derecho fundamental a la protección de datos personales y privacidad. En particular, dicha información debe servir para que los titulares de los datos sean conscientes del derecho que tienen, su significado y alcance;
6. *Las autoridades garantes tienen que colaborar con los proveedores.* En el diseño y adopción de medidas, como por ejemplo planes sectoriales dirigidos a los proveedores de telecomunicaciones e Internet, así como buscar formas y mecanismos de colaboración con los proveedores, para considerar así todos los aspectos que se plantean en relación con el tratamiento de datos personales y la prestación de servicios de telecomunicaciones e Internet. Sin dicha colaboración se podrían producir situaciones de desequilibrio que son perjudiciales para todas las partes, ya que se podría limitar de manera indebida la innovación tecnológica, privando de importantes beneficios a los usuarios, o se podría dar lugar a una situación en la que no se proteja de manera efectiva el derecho fundamental a la protección de datos personales;
7. *Las autoridades garantes deben colaborar también con otras autoridades.* Una protección efectiva de los titulares de los datos personales implica que las autoridades garantes tengan

que considerar la necesidad de colaborar con otras autoridades garantes o, en su caso, competentes en otras áreas que están interrelacionadas con la protección de datos personales. Siendo la protección de datos personales una cuestión transversal, la cooperación entre autoridades es fundamental, de manera que acciones coordinadas, ya sean con carácter general o dirigidas a sectores específicos como por ejemplo el de telecomunicaciones o servicios relacionados con Internet, son importantes;

8. *Las autoridades garantes deben desarrollar planes o políticas públicas sobre protección de datos personales que incluyan a todas las partes interesadas.* En caso de que una autoridad garante elabore instrumentos o medidas, tales como planes o políticas públicas, para fomentar la protección de datos personales, es importante que se cuente con la colaboración de todas las partes interesadas para garantizar así que se tienen en consideración todos los aspectos que se plantean y que no se da lugar a planes o políticas públicas que no son efectivas por no considerar todos los aspectos o cuestiones necesarias;
9. *Las autoridades garantes deben vigilar el cumplimiento de la normatividad.* Puesto que el incumplimiento de la misma implica, entre otros aspectos, que se produzca una vulneración del derecho fundamental a la protección de datos personales, de manera que es necesario que se impongan sanciones efectivas que disuadan de volver a cometer infracciones a quienes no cumplen con dicha normatividad. Además, velar de manera constante por el cumplimiento de la normatividad puede ayudar a identificar puntos débiles así como buenas prácticas que sirvan para adoptar o, en su caso, proponer otras medidas;
10. *Las autoridades garantes tienen que desarrollar y mantener acciones a lo largo del tiempo.* No resulta suficiente con adoptar medidas en y para un momento determinado, sino que es necesario que se mantengan a lo largo del tiempo para que sean así efectivas a largo plazo. Es importante que las autoridades garantes aborden la protección de datos personales como un objetivo a largo plazo que requiere la adopción de medidas durante el trayecto, especialmente a la vista de la evolución tecnológica y de los cambios sociales, económicos y de otra naturaleza que se van produciendo.

Referencias bibliográficas

Álvarez Caro, María, "Reflexiones sobre la sentencia del TJUE en el asunto 'Mario Costeja' (C-131/12) sobre derecho al olvido", *Revista Española de Derecho Europeo*, núm. 51, pp. 165-187.

Cate, Fred H., Peter Cullen y Viktor Mayer-Schönberger (2014), *Data Protection Principles for the 21st Century, Revising the 1980 OECD Guidelines*. Disponible en <http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf>.

Cate, Fred H. y Viktor Mayer-Schönberger (2013), *Data use and impact global workshop*. Disponible en <http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf>.

Doneda, Danilo (2014), *Privacy and data protection in the Marco Civil da Internet (Brazilian Civil Rights Framework for the Internet Bill)*. Disponible en <http://www.privacylatam.com/?p=239>.

European Data Protection Supervisor (2014), *Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*. Disponible en <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf>.

Federal Trade Commission (2012), *Protecting Consumer Privacy in an Era of Rapid Change, A proposed framework for businesses and policymakers*. Disponible en <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

Foro Económico Mundial (2014), *Delivering Digital Infraestructure: Advancing the Internet Economy*. Disponible en <http://www3.

weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf>.

_____ (2014), *Rethinking Personal Data: A New Lens for Strengthening Trust*. Disponible en <http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf>.

_____ (2014), *Rethinking Personal Data: Trust and Context in User-Centered Data Ecosystems*. Disponible en <http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf>.

Gregorio, Carlos G. y Lina Ornelas Núñez (2011), *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo*, México, IIJusticia/IFAI.

Maqueo, María Solange y Jimena Moreno (2014), *Implicaciones de una ley general en materia de protección de datos personales*, México, CIDE. Disponible en <http://www.cide.edu/publicaciones/status/dts/DTEJ%2064.pdf>.

Murillo de la Cueva, Pablo Lucas y José Luis Piñar Mañas (2009), *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo.

Organización para la Cooperación y el Desarrollo Económicos (2011), *Thirty years after the OECD Privacy Guidelines*.

_____ (2012), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, núm. 211, OECD Publishing. Disponible en <http://dx.doi.org/10.1787/5k8zq92vdgtl-en>.

_____ (2012), "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy

and the Protection of Children Online", *OECD Digital Economy Papers*, núm. 214, OECD Publishing. Disponible en <http://dx.doi.org/10.1787/5k4dq3rkb19n-en>.

_____ (2014), *Data-driven Innovation for Growth and Well-being, Interim Synthesis Report*. Disponible en <http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf>.

Piñar Mañas, José Luis y Lina Ornelas Núñez (2013), *La protección de datos personales en México*, México, Tirant lo Blanch.

Piñar Mañas, José Luis y Miguel Recio Gayo (2013), *Código de protección de datos personales México*, México, Tirant lo Blanch.

Recio Gayo, Miguel (2013), *Esquemas de la Ley de protección de datos personales y su reglamento*, México, Tirant lo Blanch.

Warren, Samuel D. y Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, vol. IV, núm. 5, 5 de diciembre de 1890. Disponible en <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

Westin, Alan F. (1966), "Science, Privacy, and Freedom: Issues and proposals for the 1970´s", *Columbia Law Review*, vol. 66, p. 1003.

_____ (1967), *Privacy and Freedom*, Nueva York, Atheneum.

White House (2012), *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Disponible en <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

Acuerdo mediante el cual la Procuraduría Federal del Consumidor y el Instituto Federal de Telecomunicaciones, determinan los derechos mínimos que deben incluirse en la carta a que hace referencia el artículo 191 de la Ley Federal de Telecomunicaciones y Radiodifusión. Disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5399492&fecha=06/07/2015>.

Asociación Mexicana de Internet (AMIPCI) (2015), Estudio de Comercio Electrónico en México 2015. Disponible en <https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf>.

Constitución Política de los Estados Unidos Mexicanos. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/1_07jul14.pdf>.

Dictamen de la Comisión de Gobernación con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Disponible en <http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf>.

Gobierno de la República (2014), Reforma en materia de telecomunicaciones. Disponible en <http://reformas.gob.mx/wp-content/uploads/2014/06/EXPLICACION_AMPLIADA_DE_LA_REFORMA_EN_MATERIA_DE_TELECOMUNICACIONES.pdf>.

Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE (1999), *Documento de trabajo: Tratamiento de datos personales en Internet*, WP 16. Disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp16_es.pdf>.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.

Ley Federal de Telecomunicaciones y Radiodifusión. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_140714.pdf>.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf>.

Sentencia del Tribunal de Justicia de la Unión Europea, 6 de noviembre de 2003, "Directiva 95/46/CE – Ámbito de aplicación – Publicación de datos personales en Internet – Lugar de la publicación – Concepto de transferencia de datos personales a países terceros – Libertad de expresión – Compatibilidad con la Directiva 95/46 de una protección más rigurosa de los datos personales por parte de la normativa de un Estado miembro", en el asunto C-101/01. Disponible en <http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=337168>.

Sentencia del Tribunal de Justicia (Gran Sala), 13 de mayo de 2014, "Datos personales – Protección de las personas físicas en lo que respecta al tratamiento de dichos datos – Directiva 95/46/CE – Artículos 2, 4, 12 y 14 – Ámbito de aplicación material y territorial – Motores de búsqueda en Internet – Tratamiento de datos contenidos en sitios de Internet – Búsqueda, indexación y almacenamiento de estos datos – Responsabilidad del gestor del motor de búsqueda – Establecimiento en territorio de un Estado miembro – Alcance de las obligaciones de dicho gestor y de los derechos del interesado – Carta de los Derechos Fundamentales de la Unión Europea – Artículos 7 y 8", asunto C-131/12. Disponible en <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=531281>.

Sitios en Internet

Asociación Mexicana de Internet (AMIPCI), <https://www.amipci.org.mx>.

Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), <http://www.infodf.org.mx>.

Instituto Federal de Telecomunicaciones (IFT), <http://www.ift.org.mx>.

Instituto Nacional de Estadística y Geografía (INEGI), <http://www.inegi.gob.mx>.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), <http://www.inai.org.mx>.

México Conectado, <http://mexicoconectado.gob.mx>.

Procuraduría Federal del Consumidor (Profeco), <http://www.profeco.gob.mx>.

Red Iberoamericana de Protección de Datos, <http://www.redipd.org>.

Colección Ensayos para la Transparencia de la Ciudad de México

2007

01 **La transparencia y los sujetos no obligados de la rendición de cuentas.** Alberto Aziz Nassif

02 **Archivos gubernamentales: un dilema de la transparencia**. José Antonio Ramírez Deleón

03 **Transparencia y control ciudadano: comparativo de grandes ciudades**. Irma Eréndira Sandoval

2008

04 **¿Por qué transparentar las actividades de cabildeo? El caso del Presupuesto de Egresos de la Ciudad de México.** Alejandra Betanzo de la Rosa

05 **Transparencia y procuración de justicia en el Distrito Federal.** Catalina Pérez Correa González y Alejandro Madrazo Lajous

06 **Acceso a la información y transparencia política en el Distrito Federal.** Issa Luna Pla

07 **El derecho de acceso a la información pública: una herramienta para el ejercicio de los derechos fundamentales.** Paulina Gutiérrez Jiménez

08 **Transparencia y medios de comunicación.** Marco A. Morales Barba

2009

09 **Hacia una nueva arquitectura de la información pública. Información pública y política social en el Distrito Federal.** Eduardo Bohórquez

10 **Legislar en la oscuridad. La rendición de cuentas en la Asamblea Legislativa del Distrito Federal.** Khemvirg Puente

11 **Construir obra pública, edificar ciudadanía.** Miguel Ángel Pulido Jiménez

12 **Las delegaciones y los servicios públicos: una mirada sobre lo que deberíamos saber.** Darío Ramírez Salazar y Gabriela Morales Martínez

2010

13 **Sindicatos y transparencia en la Ciudad de México.** Arturo Alcalde Justiniani

14 **Transparencia 2.0 Nuevos medios digitales y acceso a la información pública en el Distrito Federal, oportunidad para el empoderamiento ciudadano.** Octavio Islas y Mauricio Huitrón

15 **Transparencia y desarrollo urbano en el Distrito Federal.** Emilio de Jesús Saldaña Hernández

2011

16 **La libertad de expresión y el derecho a la información en México: un desafío de nuestros tiempos.** Emilio Álvarez Icaza Longoria

17 **Transparencia y procesos electorales.** Lorenzo Córdova Vianello

18 **Acceso a la información, periodismo y redes sociales, escenarios futuros.** Jenaro Villamil

19 **Transparencia, acceso a la información y participación social en la ciudad de México.** Ricardo Raphael

2012

20 **Acceso a la información y protección de datos personales en el ámbito de la justicia.** Miguel Carbonell

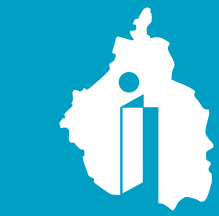
21 **Transparencia y gobierno abierto en el D.F., ¿Para qué?.** Haydeé Pérez Garrido

2013

22 **Transparencia y gastos de campaña en las elecciones: dos eslabones para la legalidad y la legitimidad electoral en la ciudad de México.** Manuel Larrosa Haro

23 **El derecho al olvido en relación con el derecho a la protección de datos personales.** Isabel Davara Fernández De Marcos

24 **La protección de datos personales de menores en la era digital.** Lina Gabriela Órnelas Núñez y Samantha Alcalde Urbina



Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Ensayo 25 "La protección de datos en el ámbito de las telecomunicaciones e internet"

Diciembre 2015

xxxxxxxx xxxxxx xxxxxx
xxxxx xxxxxxxxxx xxxxxxx xxx
xxxxxxxx xxxxxxx xxxxxxxxxx xxxxxxxx
xxxxxxxx xxxxxxx xxxxx

El tiraje fue de 1,000 ejemplares impresos en papel bond de 90 grs. Y forros en couché de 250 grs. Fuentes tipográficas: (Calibri Regular, Calibri Bold, Calibri italic, Myriad ProRegular y Myriad ProSemibold)
Cuidado de la edición: Dirección de Capacitación y Cultura de la Transparencia