INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO

POSGRADOS

"RECOMENDACIONES DE PROTECCIÓN JURÍDICA PARA LOS DATOS PERSONALES RESPECTO AL REGISTRO Y LA CONSERVACIÓN, REALIZADOS DE CONFORMIDAD CON EL ARTÍCULO 190, FRACCIÓN II DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN"

SOLUCIÓN ESTRATÉGICA EMPRESARIAL
Que para obtener el grado de MAESTRO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Presenta:

Lic. Sergio Rangel Garrocho

Asesor:

Dr. Alberto Enrique Nava Garcés

Ciudad de México, Abril de 2018.

Autorización de Impresión

INFOTEC POSGRADOS

C4

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 04 de mayo de 2018

La Gerencia de Capital Humano/ Gerencia de Investigación hacen constar que el proyecto terminal titulado:

"Recomendaciones de protección jurídica para los datos personales respecto al registro y la conservación, realizados de conformidad con el artículo 190, Fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión"

Desarrollada por el alumno

Nombre: **Sergio**

Apellido paterno: **Rangel**

Apellido materno: **Garrocho**

Desarrollado bajo la asesoría del:

Dr. Alberto Enrique Nava Garcés

Ha sido revisado y aprobado por miembro del Núcleo Académico Básico (NAB).

Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

Mtra. Patricia Ávila Muñoz
Gerencia de Capital Humano

*Anexar a la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.

Agradecimientos

Dedico esta obra a mi hermosa familia, Alejandra, Emilio, Alejandro, Herlinda, Sergio, Samuel, Siegsfried, Claudia, Nataly, Flavio, Sarahí, María y Thania.

A mis maestros les agradezco su enseñanza e impulso y a mi asesor de esta obra, le doy gracias por su guía y apoyo incondicional.

A mis amigos involucrados en esta nueva etapa, mi reconocimiento y admiración por estar a la vanguardia y hacerme partícipe de los grandes cambios.

A mis amigos que han aportado su apoyo de una u otra forma para concluir este proyecto, les agradezco formar parte de mi vida y estar en esos momentos trascendentales.

Tabla de contenido

Índice de figuras

Índice de cuadros

Siglas y abreviaturas

IoT. Internet de las cosas.

ISP. Proveedor de acceso a Internet, por sus siglas en inglés.

Firewall. Equipo o software de seguridad.

TIC. Tecnología de la información y comunicaciones.

LFTR. Ley Federal de Telecomunicaciones y Radiodifusión.

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

SGSDP. Sistema de gestión de la seguridad de datos personales.

OCDE. Organización para la Cooperación y el Desarrollo Económico.

SCJN. Suprema Corte de Justicia de la Nación.

IFT. Instituto Federal de Telecomunicaciones.

INAI. Instituto Nacional de Acceso a la Información Pública Gubernamental y Protección de Datos.

GNI. The Global Network Initiative.

Introducción

Los datos conservados por los Concesionarios constituyen en conjunto información digital susceptible ataques motivados por su valor económico.

El acceso no autorizado a las bases de datos de registro y control, o el sabotaje que interrumpe el normal funcionamiento de los sistemas y redes de información, son los principales riesgos que la tecnología trae consigo en un mundo interconectado[1]. La posibilidad de que algún tercero se aproveche de una vulnerabilidad que nos ubique en cualquiera de ambos supuestos, también tiene cabida real en la conservación de datos para colaboración con la justicia.

Estos riesgos pueden surgir de fuentes externas o de fuentes internas. Por ello, los concesionarios deben diseñar sus sistemas de conservación de datos digitales, y su proceso de entrega a las autoridades (ya sea en forma física o digital), considerando siempre las posibles amenazas para la información conservada, tanto internas como externas.

El objetivo de las recomendaciones consiste en que a través de su ejecución se protejan los derechos fundamentales de los usuarios durante la conservación de los datos personales que realizan los Concesionarios y con ello, asegurar el valor público de los metadatos, a través de la entrega efectiva y oportuna de éstos a las autoridades competentes[2].

---

[1] David Chinn, et al, Risk and responsibility in a hyperconnected world: Implications for enterprises McKinsey&Company, enero 2014., página 2. Archivo PDF consultado el 16 de diciembre de 2015 en http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises

[2] Conforme al Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996, para la gestión de la entrega oportuna y efectiva podrían intervenir las autoridades designadas para la gestión o las autoridades

En el primer capítulo abordaremos los temas que explican cómo es que la tecnología está inmersa en los aspectos cotidianos de la vida, la importancia de la economía digital y las razones por las cuales los registros de las comunicaciones de los usuarios, son valiosos en la persecución e investigación de delitos. Al terminar este capítulo advertiremos la importancia de la información personal digitalizada en los sistemas y redes de información, así como, la problemática que representa para los concesionarios de telecomunicaciones proteger jurídica y técnicamente la información personal de sus usuarios, que es conservada mediante el registro de las llamadas realizadas por éstos a través de sus teléfonos móviles o fijos.

Con motivo de la nueva regulación a los Concesionarios se les obliga a crear una base de datos de las comunicaciones de los usuarios, controlar su acceso y ante la solicitud de una autoridad facultada, entregar los registros de las llamadas para la investigación y persecución de delitos, sin embargo, no está claro cuáles son las directrices que deben seguir los concesionarios, para proteger la información personal mientras es conservada durante el periodo establecido en la ley, en consecuencia, se vuelve complejo definir la mejor práctica para mantener la expectativa de respeto a la vida privada de los usuarios de estos servicios de comunicaciones.

Si bien es cierto, la LFTR y los Lineamientos obligan a los concesionario a utilizar la LFPDPPP, como una herramienta que guía la forma en que los concesionario deben proteger los datos personales y la vida privada de los usuarios, el cumplimiento de los principios establecidos en la misma parece diluirse porque aunque existe consentimiento de los usuarios para el tratamiento relacionado con la facturación y consumos de los servicios de telecomunicaciones, la conservación de los metadatos de sus comunicaciones electrónicas, por ministerio de ley, desborda el consentimiento otorgado por el usuario. Esta situación coloca a los concesionarios en una posición de responsabilidad frente a los usuarios, respecto

---

facultadas para requerir la información. De conformidad con el segundo lineamiento, fracciones II y III del Acuerdo en comento.

al uso legítimo de la información personal que conservarán, que los constriñe a informar de la conservación por ministerio de ley y a conocer la cadena de valor de las tecnologías de la información y comunicaciones para ubicar el eslabón que ocupan y no sólo eso, además el lugar en el que se encuentran las bases de datos de las que se obtienen los registros de las comunicaciones, para así también identificar la cadena de valor de la conservación de datos con propósitos de colaboración con la justicia que nos permita conocer la fuente de la cual se extraerán los registros de las comunicaciones de los usuarios, para que finalmente, sólo a las autoridades competentes les sea entregada la información personal solicitada.

En el segundo capítulo nos enfocaremos directamente en los aspectos de la cadena de calor de las tecnologías de información y comunicaciones, así como en los aspectos de negocio relacionados con las bases de datos que conservan la información personal de los usuarios que realizan llamadas telefónicas. El objetivo de ello es identificar la fuente de la cual se extraerán la información personal que será entregada a las autoridades, así como el valor público que existe en el cumplimiento de los principios en materia de protección de datos personales, y finalmente, la importancia de atender el deber de seguridad sobre los mismos. Comenzaremos a dar recomendaciones que tendrán eco en el tercer capítulo.

Por último, en el tercer capítulo analizaremos las medidas regulatorias concretas que prevén la conservación, registro y control de la información personal (metadatos). Realizaremos un análisis del cumplimiento a los principios en materia de protección de datos personales. A continuación, recomendaremos los estándares previstos en la regulación emitida por las autoridades para proteger la información personal. De la mano con esos estándares, propondremos un modelo que representa la cadena de valor en la conservación con propósitos de colaboración con la justicia, así como una explicación de ejecución del mismo.

Al final de este trabajo, advertiremos la recomendación consistente en la elaboración de un plan de trabajo y seguimiento que recoja todas las recomendaciones y que culmine con el deber de informar a los usuarios sobre el cumplimiento a las medidas regulatorias. Culminaremos con las conclusiones derivadas de la investigación, que consisten en recomendaciones en sí mismas y

que al ser ejecutadas, generan no sólo el cumplimiento a la regulación, sino un diferenciador competitivo en beneficio de la imagen corporativa y responsabilidad social del concesionario.

Capítulo 1

El volúmen de datos generados por interacciín con las TIC y su entrega a las autoridades

Capítulo 1: El volumen de datos generados por la interacción con las TIC y su entrega a las autoridades

1.1 Importancia de la tecnología e internet en la sociedad

Los grandes cambios en una sociedad están marcados, principalmente, por modificaciones profundas en las formas de generar riqueza. En el pasado la agricultura y la posesión de la tierra eran el factor fundamental, después, la industrialización, los medios de producción y el nacimiento de la burguesía tomaron el papel protagónico. Dentro de este proceso de evolución vemos que hay una relación directa entre la creación de riqueza y el uso de la tecnología[3].

Es natural que la tecnología sea utilizada transversalmente para hacer más eficiente a una sociedad en su conjunto. Sus efectos los vemos en los servicios que presta el gobierno, en todos los sectores industriales y sus procesos, así como en la forma en que los individuos nos comunicamos. El desarrollo económico en cualquier sociedad ha sido impulsado en gran medida por los avances tecnológicos.

Las redes telefónicas tradicionales[4] son un buen ejemplo para mostrar los aspectos positivos de la tecnología. La telefonía nos ha permitido comunicarnos a distancia, lo que implica ahorros en costos asociados a los traslados. Por su parte, las computadoras han impulsado el procesamiento automatizado de la información para la toma de decisiones, hasta el punto de considerar que el uso de las

---

[3] Ruiz, Bennett, et al, “The New Digital Economy. How it will transform business”, Oxfor Economics, Research paper produced in collaboration with AT&T, Cisco, Citi, PwC & SAP. June, 2011. página 6.

[4] Aunque hay varias características que distinguen a estas redes, para los fines de este trabajo es importante resaltar que este tipo de tecnología utiliza la conmutación de circuitos, típicamente para hacer llamadas de voz. Esto significa que al hacerse una llamada se utiliza un circuito continuo desde un teléfono hasta otro, por lo que mientras se ocupe ese circuito nadie más puede utilizarlo. Para mayor información consúltese Álvarez del Castillo, Clara Luz. Internet y Derechos Fundamentales, Porrúa, México 2011, página 7.

computadoras conectadas en sistemas de información dentro de las organizaciones, es un elemento esperado y natural para la toma de decisiones.

No hace mucho y antes de la presencia de las redes de nueva generación[5] que hoy comunican a gran parte del mundo, los sistemas de información en las organizaciones se caracterizaban por funcionar en forma aislada de otros de la misma naturaleza, pues no estaban interconectados, no tenían capacidad de comunicarse ni entenderse entre sí[6].

En este paradigma, la seguridad y la protección de datos dependía del grado de aislamiento del sistema de información, mientras más aislado del mundo se encontrará menos comprometido estaría frente a las amenazas externas[7]. En este modelo el principal riesgo lo encontrábamos en las amenazas dentro de la propia organización. Los procesos económicos, de negocio, la prestación de servicios públicos y la interacción entre las personas, tampoco se daba por un medio común, de modo que los datos y la información producida dentro de dichos sistemas, no era compartida.

---

[5] Estas redes evolucionan a las redes telefónicas tradicionales pues sustituyen la conmutación física de circuitos, por la conmutación de paquetes, lo que permite dividir la información y enviarla por cualquier circuito en paquetes digitales (unos y ceros) que incluyen la voz, imágenes, documentos o videos. Debido a las redes de nueva generación, por ejemplo podemos utilizar la línea telefónica de la casa para hacer llamadas, conectarse a internet y ver videos, cuando en el pasado sólo podíamos hacer una llamada telefónica que ocupaba todo el circuito. El elemento común de estas redes es el uso del mismo lenguaje (protocolos de internet) y el aumento de la capacidad de transmisión de información digitalizada en paquetes.

[6] OECD (2012), “The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy”, OECD Digital Economy Papers, No. 209, OECD Publishing, página 5. Consultado el día 31 de diciembre de 2014 en http://dx.doi.org/10.1787/5k8zq930xr5j-en

[7] Por ejemplo las intromisiones o sustracción no autorizadas a los sistemas informáticos, la fuga de propiedad intelectual, etc.

El cambio de miles de sistemas informáticos aislados en silos, a una sociedad global de redes interconectadas, se ha dado conforme las redes de nueva generación y las computadoras se han integrado en sistemas de información más complejos comunicados a través de un mismo lenguaje técnico (protocolo TCP/IP). En ese sentido, el concepto conocido como "tecnologías de la información y la comunicación" (en adelante las TIC), fue acuñado con motivo de la convergencia tecnológica que integró a: ***(i)*** los sistemas informáticos[8] que son utilizados para almacenar y procesar los datos; y ***(ii)*** a las redes de comunicaciones de nueva generación[9] que ponen en contacto a los individuos y organizaciones separados por la distancia.

Cuando son utilizadas adecuadamente, las TIC potencializan la velocidad con la que nos comunicamos y compartimos información. Además, permiten conservar y transmitir los datos a cualquier parte del mundo en donde exista una conexión a las redes de información, especialmente a internet.[10] Su aprovechamiento ha generado disrupción, automatización y procesos de innovación, provocando cambios que han impactado en la sociedad de que se trate,

---

[8] Los sistemas informáticos están integrados típicamente por herramientas informáticas de software y también hardware.

[9] Las redes están integradas por medios de transmisión (hilos o espectro) y equipos con inteligencia para enviar la señal al destino respectivo a través de la conmutación de paquetes. Para profundizar sobre este tema consúltese a Álvarez, González de Castilla, Clara Luz, "Derecho de las Telecomunicaciones" 2da, Libertad de expresión, Unam Posgrado, 2013, Puebla, México, página 25.

[10] Internet en la opinión del Dr. Nava Garcés al citar a Jorge Vasconscelos Santillan, señala que internet *"es un conjunto de elementos tecnológicos que permiten enlazar masivamente redes de diferentes tipos para que los datos puedan ser transportados de una a otra red"*. Cfr. Nava Garcés, Alberto E. Delitos Informáticos. 2da. Porrúa, 2007, página 18.

en la medida en que penetran en casi todas las actividades de interés económico, educativo, social y público[11].

En ese sentido, la OCDE ha postulado que vivimos en un mundo interconectado donde el internet forma parte de la infraestructura operativa de sectores estratégicos como energía, transportes y finanzas de los países. Las ventajas en eficiencia de esta tecnología han influido al mundo profundamente, provocando que los individuos y organizaciones interactúen a través de las TIC al realizar todo tipo de transacciones comerciales, facilitando a su vez, que los gobiernos cumplan con sus funciones de interés público, como la seguridad y justicia, y que los ciudadanos se comuniquen e intercambien información entre ellos[12].

Al respecto, es natural que cada día haya más usuarios de internet (2900 millones)[13], que se conectan a través de equipos móviles que integran funciones de una forma cada vez más compleja. Debido a ello, el internet móvil está posicionándose como una de las tecnologías disruptivas de nuestros tiempos, que genera una gran cantidad de datos por cada llamada, descarga de contenido o aplicaciones, conexión a la red, consulta de sitios, envío de imágenes, videos, etc..

Además, no sólo las personas a través de sus dispositivos móviles, sino que los procesos de negocio y de producción, así como una variedad de sensores y equipos automatizados, se conectan cada vez en mayor número a internet. Este fenómeno es llamado el “internet de las cosas” (IoT), cuyo valor de oportunidad, a

---

[11] De hecho el internet (la red mundial) es consecuencia natural de la convergencia tecnológica. Desde nuestra perspectiva el internet y toda la tecnología asociada a éste, es el ejemplo más claro y tangible de lo que representan las TIC hoy en día.

[12] Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad, 2002, página 6., consultadas el día 27 de noviembre de 2014 en http://www.oecd.org/internet/ieconomy/34912912.pdf

[13] UIT Key ICT indicators for developed and developing countries and the world (totals and penetration rates), consultado el 15 de diciembre de 2014 en http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

decir de la empresa Cisco, representará 19 trillones de dólares durante los próximos 9 años (hasta 2024), que se verán reflejados en mayor rentabilidad de negocio, mejores servicios para los ciudadanos e incremento de ingresos en el gobierno[14].

Finalmente, existen estudios especializados en los que se advierte desde un punto de vista estadístico, por qué las TIC –incluyendo a internet- son relevantes para el desarrollo de una nación. En dichos estudios se dice que hay una correlación entre el índice de madurez digital en un país determinado y el incremento en el ingreso per cápita neto, así como en el nivel de los estándares de vida de la población.[15]

Por lo anterior, es cada vez más importante garantizar el uso legítimo y los aspectos de seguridad de la información, principalmente, la de carácter personal que constituye el insumo esencial de las TIC, sin el cual carecerían de razón de ser. La confianza en la tecnología es el factor fundamental para continuar fomentado su uso en nuestra sociedad.

1.2 La importancia de la protección jurídica de los datos personales y la privacidad en el contexto digital.

Los conceptos de privacidad y protección de datos personales, son dinámicos, evolucionan en función de las nuevas tecnologías que permiten divulgar aspectos de las personas y de su vida; desde la escritura hasta el internet estos conceptos han cambiado con cada adelanto de la ciencia. Lo que hace poco era considerado

[14] Bradley, Joseph, et al, Internet of Everything (IoE) Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector. Puede consultarse en http://www.cisco.com/web/about/ac79/docs/IoE/IoE-VAS_Public-Sector_Top-10-Insights.pdf

[15] Pélissié du Rausas Matthieu, et al. "Internet matters: The Next sweeping impact on growth, Jobs, and prosperity", McKinsey Global Institute, mayo 2011. Consultado el 27 de noviembre de 2014 en http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters

una vulneración a la vida privada, como tomar o publicar una fotografía[16], hoy en ciertos contextos ya no lo es. En la actualidad, los datos que identifican a una persona están representados por datos digitales conservados en los sistemas de información que integran las TIC, cuya funcionalidad consisten en el procesamiento y uso compartido con fines, por ejemplo, de negocio o interés público, generando resultados que revelan el comportamiento, los gustos, la psicología, etc. de los usuarios de las TIC.

Efectivamente, al usar las TIC, la información que identifica a los individuos por los datos que generan (comportamiento, ubicación, hora día y con quien se comunican) queda registrada en los sistemas y redes de información.

Con motivo de la conservación y el uso que las organizaciones dedicadas a explotar las TIC, puedan dar a los datos, existe un riesgo potencial de afectación a la privacidad y datos de los usuarios, principalmente por la pérdida de control y capacidad de proteger su información cuando ésta es generada, o en su caso, migra a un formato digital por la interacción de los individuos con las TIC.[17]

Los servicios prestados a los usuarios de las TIC en los nuevos modelos de negocio o de gobierno, que son habilitados por el cómputo en la nube, el análisis de grandes bases de datos, el espionaje cibernético, la capacidad de correlacionar datos, cosas (sensores y actuadores) que se conectan a internet, la comunicación móvil, así como las redes sociales; deben ser considerados conductores de riesgo para la privacidad y datos personales de los usuarios que interactúan con las redes y sistemas de información. El uso de la tecnología implica compartir la información personal, sin conocer las capacidades técnicas de las TIC y ni los usos futuros que

[16]La toma de una fotografía es uno de los hechos que se analiza en este famoso ensayo sobre el derecho a la privacidad. Samuel D. Warren y Louis D. Brandeis, “The Right to Privacy”, Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890).

[17] The APEC Privacy Framework, página 6, consultado el día 16 de febrero de 2015. http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

estas tecnologías permiten darle a la información personal que generan los usuarios.

Paradójicamente, el valor de los datos digitalizados radica en su integridad, disponibilidad y confidencialidad para poder ser objeto de análisis, así como para evitar la afectación a la privacidad de las personas, pues un dato personal falso o que es alterado no es útil y en cambio, puede traer consecuencias inesperadas porque puede inducir a errores. La importancia de la protección a la privacidad y datos personales en el contexto digital, radica en que sólo de su mano se asegura la confianza en el uso de las TIC y todas las consecuencias positivas que derivan de ellas.

1.3 Clasificación de los datos digitales

Intentar distinguir claramente los datos que integran la información es complejo, sin embargo, podemos aproximarnos a una clasificación general: ***(i)*** los datos comunes, los cuales son de acceso público o con mínimos requisitos para su acceso, ***(ii)*** los datos propietarios incluyendo la propiedad intelectual y los datos personales[18] cuyo control legal y tecnológico le corresponde a los individuos y a las organizaciones, que pueden ser objeto de auditoría y ***(iii)*** los datos del gobierno, que tienen menos supervisión pública y controles estrictos de uso[19].

Además, en términos generales existen ciertos datos que identifican otros datos que conocidos como metadatos, los cuales se ubican en los incisos (ii) y (iii) antes mencionados. Estos datos ofrecen la oportunidad de referirnos a algunas de las técnicas y tecnologías aplicadas a su análisis para generar valor de negocio o valor público; éstas pertenecen a diversos campos de la ciencia como la estadística,

---

[18] Bailey, Tucker, et al, “Playing war games to prepare for a cyberattack”, McKinsey Global Institute, Julio, 2012. Consultado el día 27 de noviembre de 2014 en http://www.mckinsey.com/insights/business_technology/playing_war_games_to_prepare_for_a_cyberattack

[19] Pentland, Alex, “Big Data: Balancing the Risks and Rewards of Data-Driven Public Policy”, The Global Information Technology Report 2014, Rewards and Risks of Big Data, World Economic Forum, pagina 53

computación, matemáticas aplicadas y economía; su fin es encontrar correlaciones y patrones entre datos, así como, realizar inferencias entre éstos.[20]

Es una realidad que los individuos y las organizaciones mantienen una conexión permanente a la internet a través de sus dispositivos y una relación cada vez más profunda con las TIC. Esta interacción reiterada de los usuarios, tiene un impacto directo en el aumento de la cantidad de datos digitales (información personal o de negocio), que se genera constantemente. La información que circula en las redes y sistemas de información, es el insumo principal de las TIC.

En relación con ello, un estudio reciente de la empresa EMC sostiene que la cantidad de datos generados en el mundo en el año 2011, se estimó en 1.8 zettabytes (1.8 trillones de gigabytes), de los cuales el 75% fue generado por los usuarios. De ese universo de datos, alrededor de un tercio contaba con las medidas mínimas de seguridad y protección contra el uso ilegítimo.[21] Esta estadística es crítica si pensamos en la importancia de los datos digitales y la necesidad de que sean protegidos para fomentar el uso de la tecnología.

1.4 Los metadatos y las implicaciones para la privacidad de los usuarios

Los metadatos son los datos que describen los registros generados al utilizar las tecnologías de la información, sirven para identificar cualquier dato de la clasificación hecha en el anterior subtema[22]. En el caso de las llamadas telefónicas,

---

[20] Manyika, James, et "Big data: The next frontier for innovation, competition, and productivity", McKinsey & Company 2011, página 27.

[21] Gantz, John and Reinsel, David, "Extracting Value from Chaos", Sponsored by EMC Corporation, junio 2011, consultado el 1 de febrero de 2015 en http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf

[22] El concepto de metadata puede ser aplicado a la creación de un documento, el hacer una llamada telefónica, generar un documentos en word o tener una comunicación a través de una dirección IP, en este trabajo nos referiremos

los metadatos [23] pueden ser utilizados para hacer modelos de las conexiones sociales de los usuarios de un número telefónico y de sus contactos[24]. Los metadatos se generan por cada comunicación, son el rastro que perdura después de que se realizó una llamada a través de una línea.

Los metadatos permiten describir el contexto en el que se realizó una llamada telefónica (fecha, hora, lugar y usuario), por ejemplo, las llamadas que se hacen a través de cualquier línea de teléfono o mediante el uso de una dirección IP[25]

---

principalmente a los metadatos de las comunicaciones realizadas por una línea telefónica.

[23] Tauberer, Joshua, "What is RFD". Traducción nuestra: Joshua Tauberer explica que los metadatos son "los datos de los datos". Los Metadatos es … información en algun sentido secundaria a los datos que estan en la red. "metadata--literally, data about data. Metadata is, … information that is in some sense secondary to some other content already on the regular web", consultada el día 29 de Julio de 2014, http://www.xml.com/pub/a/2001/01/24/rdf.html.

[24] Risen, James and Poitrassept, Laura, "N.S.A. Gathers Data on Social Connections of U.S. Citizens", The New York Times, 28 septiembre 2013, Consultada el día 29 de julio de 2014 traducción nuestra "…huge collections of data to create sophisticated graphs of some Americans social connections that can identify their associates, their locations at certain times, their traveling companions and other personal information. "…enormes bases de datos mediante las cuales se crean gráficas sofisticadas de conexiones sociales de algunos estadounidenses, que pueden identificar sus asociados, sus ubicaciones en determinados momentos y de sus compañeros de viaje y cualquier otra información personal…"
http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all&_r=1&

[25] "Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol)".

utilizando el protocolo de internet. Los resultados que arrojan las tecnologías avanzadas que analizan los metadatos, permiten saber quién llama a quién, cuándo lo hace y desde dónde lo hace, generando correlaciones entre los datos de los individuos son conservados[26], lo que permite pronosticar incluso el patrón de comportamiento de los usuarios. En una escala masiva, es posible predecir lo que los individuos de una sociedad harán en un momento determinado[27].

Consultado en https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP el 27 de agosto de 2015.

[26] Para profundizar en este tema consultar ver el video de TED talk consultable en la siguiente liga: http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching

También revisar Spitz, Malte, "Why Metadata Matters: The Dangers and Revealing Nature of Data Retention" consultado el 19 de febrero de 2015 en https://www.eff.org/node/81907

[27] Amparo en Revisión 937/2015, del índice de la Segunda Sala de la Suprema Corte de Justicia de la Nación, página 24, que a la letra señala respecto del artículo 190, fracciones I y II, que *"Al respecto, esta Segunda Sala considera que como señalan las recurrentes, se trata de una injerencia en la vida privada de las personas, pues la medida impugnada está dirigida a retener por un periodo prolongado determinada información, la cual basta para reconstruir quién realiza el proceso comunicativo, cuándo, por cuánto tiempo, con quién y desde dónde se llevó a cabo.*

Lo anterior debido a que si bien la información recabada con el almacenamiento de los datos relativos al tráfico de las comunicaciones de telefonía fija o móvil no comprende el contenido de la comunicación, lo cierto es que permite identificar no solo la identidad de los interlocutores, sino también parte de sus actividades o relaciones sociales". Consultado el día 10 de octubre de 2016 en http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=186831

Tratándose de la seguridad y persecución de delitos, la conservación masiva de los metadatos constituye una fuente de información valiosa para las autoridades estatales. Debido a ello, es necesario protegerlos jurídicamente desde su origen y durante la conservación de éstos, vigilando su uso legítimo y la seguridad que mantiene su integridad. Esta obligación de protección de la privacidad y datos personales, es clara para los concesionarios de telecomunicaciones en México, pues así se reducen los riesgos que amenazan la información personal digitalizada por ellos.

1.5 Protección holística en los sistemas de comunicación e información

La información personal generada por la interacción de los usuarios con las TIC[28] está sujeta por una parte a requerimientos de entrega al Estado[29], y por la otra, está expuesta a las amenazas internas y externas que se traducen en formas de explotación ilegítima de la información personal.

En este escenario, junto a las ventajas en eficiencia que ofrece la tecnología, viene aparejada la responsabilidad de los concesionarios frente al usuario. A este respecto, es necesario continuar tutelando la información personal, a la luz de los riesgos que acompañan a las nuevas tecnologías[30], se trata entonces de aplicar las mejores prácticas técnicas, administrativas y físicas, con la característica de ser dúctiles, para no obstaculizar el ejercicio de las facultades de las autoridades, sino apoyarlas en un ambiente tecnológico de uso legítimo y seguro de la información personal.

---

[28] Artículo 3, fracción V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[29] La entrega debe realizarse con independencia del consentimiento del usuario y sin posibilidad de que pueda oponerse a ello, por ministerio de la propia ley.

[30] Consúltese la Declaración de la CMSI+10 relativa a la aplicación de los resultados de la CMSI. Consultada el 27 de noviembre de 2014 en http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/362828V2S.pdf

Nos parece adecuado hablar de una práctica denominada “privacidad por diseño”. El enfoque de esta práctica es previo, la preocupación por proteger la privacidad y los datos personales, se encuentra inmersa en el diseño mismo de los productos o servicios de TIC. En esa medida, dado que un concesionario tendrá que diseñar e implementar procesos y sistemas de información automatizada para cumplir con la obligación de entregar los metadatos a las autoridades de acuerdo a la ley, se aprecia necesario atender las preocupaciones de protección jurídica de los datos personales desde el diseño de estos procesos y sistemas.

Los objetivos de la privacidad por diseño, son[31]: i) asegurar la privacidad, ii) obtener control personal de la información propia, y iii) para las organizaciones, obtener una ventaja competitiva sostenible.[32] La privacidad por diseño se extienden homogéneamente a una “Trilogía” de aplicaciones que engloban: 1) sistemas de tecnologías de la información; 2) prácticas comerciales responsables; y 3) diseño físico e infraestructura en red, las cuales se alcanzan a través de sus principios fundacionales.[33]

Otro objetivo de esta práctica es extender estos principios a toda la cadena de valor de las TIC. La autorregulación y las mejores prácticas que se dan a nivel internacional, son el principal medio para proteger la información personal en esta cadena.

---

[31] Cavoukian, Ann, “Privacy by Design, The Seven Fundational Principles”, consultado el dìa 22 de abril de 29017 en https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[32] Idem.

[33] Ibidem (ob cit 31). Los principios fundacionales son: 1. Proactivo, no Reactivo; Preventivo no Correctivo, 2. Privacidad como la Configuración Predeterminada, 3. Privacidad Incrustada en el Diseño, 4. Funcionalidad Total – “Todos ganan”, no “Si alguien gana, otro pierde”, 5. Seguridad Extremo-a-Extremo – Protección de Ciclo de Vida Completo, 6. Visibilidad y Transparencia – Mantenerlo Abierto, 7. Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario.

1.6 Algunos casos de vulneraciones

Sector privado. Debido a la capacidad intrusiva en la vida privada que tienen las empresas propietarias de las TIC y el Estado, se dice que hemos llegado al fin de la vida privada como nuestros abuelos la concibieron[34].

En el año 2014 los Medios informaron de la vulneración a los sistemas de información de la empresa Target, este ataque afectó a 40 millones de tarjetas de crédito y débito. De acuerdo con los comunicados de prensa, la información personal de 70 millones de usuarios pudo estar expuesta a los piratas informáticos, debido a ello se considera uno de los ataques más importantes de este tipo.[35] Por otra parte, en el caso de Google también hubo noticias acerca de un ataque cibernético perpetuado en contra de las cuentas de correo electrónico de sus usuarios, lo que pudo suceder desde una provincia china, hecho que a decir de las noticias, desató una problemática de tipo político y al mismo tiempo, paradójicamente convirtió a la Universidad Lanxiang, desde donde al parecer se llevó a cabo el ataque, en un centro de enseñanza de mayor prestigio.[36]

Sector público. Si quisiéramos tomar un caso en el que la privacidad y la protección de datos personales se vieron comprometidos, la referencia por

---

[34] Preston, Alex, “The Death of Privacy”, The Guardian, 3 de Agosto 2014, consultado el 9 de marzo de 2015 en http://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

[35] Pozzi, Sandro. “Target despide al consejero delegado tras un ataque informático”, El País, 5 de mayo de 2014, consultado el 10 de marzo de 2015 en http://economia.elpais.com/economia/2014/05/05/actualidad/1399300492_653465.html

[36] Agencias, “El escándalo da a conocer la escuela china sospechosa de los ciberataques a Google”, El país, 22 de febrero de 2010, consultado el día 10 de marzo de 2015 en http://tecnologia.elpais.com/tecnologia/2010/02/22/actualidad/1266832863_850215.html

excelencia la encontramos en los programas de investigación (FiveEyes) de la Agencia Nacional de Seguridad de los Estados Unidos, que fueron revelados por Eduard Snowden y publicados por el periódico "The Guardian"[37] a mediados del año 2013. Estos programas de espionaje, hasta donde sabemos por la revelación, conservan los metadatos de las llamadas telefónicas y del tráfico de internet generado por los usuarios de estas tecnologías, al parecer con alcances globales. Otro caso se dio en el marco del Acuerdo Nacional por la Seguridad, la Justicia y la Legalidad que fue publicado en el año 2008, por virtud del cual fue creado el Registro Nacional de Usuarios de telefonía móvil (Renaut) - en control de la Secretaría de Gobernación- cuya base de datos, según los Medios, podría haber sido comercializada a través de internet, esta filtración fue objeto de investigaciones de la Procuraduría General de la República y de la Secretaría de Gobernación.[38] Esta historia también sucedió con la base de datos del padrón electoral del Instituto Federal Electoral, respecto de la cual los medios informaron que también se encontraban a la venta.[39]

Dichos casos de los sectores público y privado relacionados con vulneraciones a los sistemas y redes de información, culminaron con la pérdida del valor de la información personal y la presencia de consecuencias inesperadas para sus titulares. Ante situaciones como éstas, es necesario evaluar la situación en el seno de la organización, sobre todo en las empresas de TIC, para identificar los perfiles de riesgo que hay al interior y exterior, y atenderlos preventivamente,

---

[37] Roberts, Dan y Ackerman, Spencer, "US intelligence outlines checks it says validate surveillance" The Guardian, consultado el 9 de marzo de 2015 en http://www.theguardian.com/world/2013/jun/16/nsa-the-nsa-files

[38] Solís, Victor, "Datos de celulares a la Venta en Web", El Universal, 3 de junio de 2010, consultado el 9 de marzo de 2015 en http://www.eluniversal.com.mx/notas/685120.html

[39] Noticias consultadas el día 9 de marzo de 2015 http://eleconomista.com.mx/sociedad/2010/04/20/pgr-investiga-venta-padron-ife-tepito, http://www.proceso.com.mx/?p=107549

aprendiendo de la experiencia de terceros quienes se vieron sorprendidos por contingencias para las que, en ocasiones, no estuvieron debidamente preparados.

1.7 Una medida regulatoria controversial

Por el crecimiento exponencial que ha tenido el internet y las comunicaciones móviles, los metadatos generados por al uso de estas tecnologías, son particularmente importantes para prevenir y perseguir los delitos. El rastro que perdura por lo general hasta tiempo después de que la comunicación se realizó, es un elemento muy valioso para las autoridades de justicia y seguridad nacional en la investigación de delitos[40].

En el caso de México, la solución a esta necesidad exigió medidas y políticas públicas enfocadas en el uso de la tecnología durante la investigación y persecución de los delitos. Naturalmente, la complejidad del escenario provoca la tensión entre derechos fundamentales, como la privacidad y protección de datos personales, y el derecho a la seguridad en la sociedad.

Precisamente, la obligación de los concesionarios de telecomunicaciones que los constriñe a colaborar con las instancias de seguridad y procuración de justicia, mediante la conservación y entrega de los metadatos de las llamadas telefónicas, genera un riesgo a la vida privada y protección de datos de sus usuarios, que se convierte en una carga regulatoria compleja que implica diseñar y ejecutar un plan de protección a la información personal en el que además de procurar la entrega oportuna de la información para que el Estado pueda cumplir con sus funciones, los concesionarios deben velar por confirmar que la autoridad que solicite la información esté legitimada y sea competente para ello, y además, dentro del marco establecido por la ley sólo entregar la información que les esté permitido con la finalidad de tutelar constantemente la expectativa razonable de privacidad de los usuarios.

---

[40] El registro de las circunstancias en las que se prestaron los servicios de TIC, en particular las llamadas telefónicas, puede arrojar indicios en una investigación del Estado, de modo que tener acceso oportuno a los registros de las comunicaciones de los usuarios, es vital para sus autoridades.

Al respecto, uno de los Títulos más polémicos de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), es el Octavo denominado “De la Colaboración con la Justicia”, en el cual se prevén las obligaciones legales a cargo de los concesionarios de telecomunicaciones y en su caso los autorizados, que los sujetan a colaborar con las instancias de seguridad, procuración y administración de justicia en la generación y conservación del registro de comunicaciones que realicen los usuarios desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, con la finalidad de identificar con precisión diversos datos generados por los usuarios[41].

Según se desprende de la exposición de motivos[42], la inclusión de esas obligaciones a cargo de los concesionarios en dicho Título de la LFTR, obedece a la preexistencia de las mismas en la anterior Ley Federal de Telecomunicaciones y a la declaración de constitucionalidad. Recientemente la SCJN declaró la constitucionalidad del artículo 190, fracción II de la LFTR, pues constituye una injerencia constitucionalmente válida a la privacidad de las personas[43].

[41] Publicada el 14 de julio de 2014 en el Diario Oficial de la Federación.

[42] Según se desprende del Dictámen sobre la Minuta de Proyecto de Decreto por el que se expide la LFTR y otros ordenamientos legales, que emitiéron las Comisiones Unidas de Comunicaciones y de Radio y Televisión de la Cámara de Senadores del Congreso de la Unión.

[43] Amparo en Revisión 937/2015, del índice de la Segunda Sala de la Suprema Corte de Justicia de la Nación, página 39.

Capítulo 2

La conservación de datos como valor de negocio y con propósitos de colaboración con la justicia

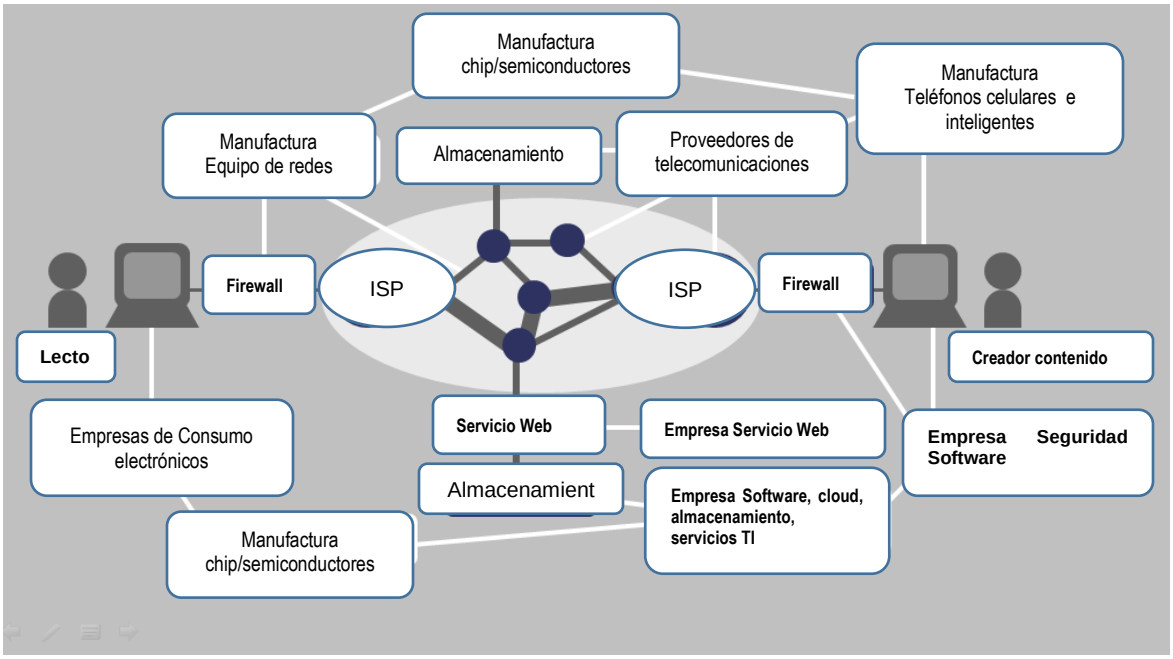
Capítulo 2: La conservación de datos como valor de negocio y con propósitos de colaboración con la justicia

2.1 La cadena de valor de las TIC

Con motivo de la convergencia tecnológica de las TIC y el incremento de ancho de banda, es posible realizar llamadas, recibir correos electrónicos, enviar mensajes, descargar videos, etc., todo a través de una misma línea contratada por el usuario de dichos servicios de telecomunicaciones. En la actualidad, mediante el uso de las TIC, es posible enviar y recibir información desde nuestros dispositivos bajo un mismo lenguaje técnico. Esta ventaja permite el flujo de información por las redes y equipos de cualquier proveedor de servicios de TIC en el mundo, incluyendo a los concesionarios de redes públicas de telecomunicaciones en México. La interoperabilidad de los equipos y sistemas (protocolos y estándares técnicos de comunicación comunes entre equipos) hace a todos los sistemas y redes de información capaces de hablarse entre sí, conectando los equipos de usuario con la red de su proveedor y las redes de otros concesionarios y con los dispositivos de otros usuarios finales. Así es como se facilita la comunicación a distancia a través de las redes, los equipos que forman parte de ellas y los equipos de los usuarios, todos bajo los mismos protocolos y estándares; que en conjunto integran una cadena de valor por la que se conectan todos los actores. En la figura se advertirá la cadena de valor de las TIC.[44] En la cadena de valor de las TIC, hay una pluralidad de actores que intervienen integrando un eslabón en la misma, cuyos actos pueden ser conductores de riesgos los datos personales de los usuarios. De tal suerte que,

[44] Allison Hope, Dunstan, "Protecting Human Rights in the Digital Age", Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry, BSR, february 2011, página 12. Consultado el 22 de abril de 2017 en https://www.bsr.org/pdfs/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf

una recomendación para los concesionarios consiste en conocer cómo está construida dicha cadena de valor, para identificar el eslabón que ocupan y de qué forma sus elementos se interrelacionan en un ecosistema de TIC, para identificar el diseño adecuado de privacidad y protección de datos que asegure la libre circulación de la información con propósitos de negocio. Todo ello, con la intención de identificar el nivel de protección a los datos personales conservados en las bases de datos generadas en los diversos modelos de negocio asociados a las TIC que tenga el concesionario[45].



ISP (Proveedor de acceso a Internet, por sus siglas en inglés)
Firewall (Equipo o software de seguridad)

Figura 1 Diagrama Cadena de Valor TIC

Fuente: Traducción propia, diagrama con base en figura propuesta en Allison Hope, Dunstan, "Protecting Human Rights in the Digital Age", Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry, BSR, february 2011, Consultado el 22

[45] Algunos de los servicios son las redes sociales, automatización de oficinas, centros de trabajo u hogares, mensajería, voz sobre IP, geolocalización, telefonía fija y móvil, etc.

de abril de 2017 en https://www.bsr.org/pdfs/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf

Ahora bien, para hacer una llamada o utilizar cualquier otro servicio de TIC, se requiere la existencia de instrucciones que identifiquen, por lo menos, el origen, destino y creador de cada comunicación para que independientemente del equipo, el mensaje pueda llegar a su destino. Sin que ello implique el conocimiento del contenido de la comunicación, estos datos de identificación se almacenan por unos meses en bases de datos creadas con ese fin (estos son los metadatos).

Con independencia de las particularidades de cada tipo de servicio de TIC, actualmente, los concesionarios de redes de telecomunicaciones, deben crear diversas bases de datos en las que registran la información personal de los usuarios y los metadatos de sus comunicaciones, con el propósito de identificar los consumos realizados por sus clientes, por ejemplo, la duración de llamada, el número telefónico de origen y destino de la llamada, la tarifa aplicable, la dirección IP de origen y destino, el ancho de banda, el nombre del usuario, datos para identificarlo, cuenta, su domicilio, entre otros.

2.2 Propósito de negocio en la conservación de los registros de las comunicaciones de los usuarios

De acuerdo con la GNI[46] existen dos niveles esenciales de información en los sistemas de las TIC y sus bases de datos. En el primer nivel, se gestiona la ruta que siguen las comunicaciones a efecto de que lleguen al destino programado. Se trata de la gestión de tráfico, gracias a la cual, como lo mencionamos en el apartado anterior, podemos hacer una llamada o enviar información a alguien específico conectado en cualquier parte del mundo. El segundo, es el nivel de contenido de la comunicación que comprende toda clase de información, ya sea de voz, escritura,

[46] The Global Network Initiative

video o sonido. En ambos casos, los datos y la información están registrados y controlados en diversas bases de datos, creadas con propósitos de negocio.

Es natural que los concesionarios conserven la información personal de los usuarios y la asocien con los metadatos generados por las comunicaciones realizadas por éstos, pues mediante esta correlación de información, pueden facturar el servicio prestado y así obtener el pago respectivo, posteriormente se borrar la información del usuario para eliminar los costos asociados a la conservación en bases de datos. Los registros y el control de las bases de datos que comentamos, nacieron al mismo tiempo que los servicios prestados a través de las TIC.

El "registro" implica la creación de una base de datos ordenada lógicamente[47]. Esta base de datos puede ser autónoma alimentada enforma independiente o derivarse de otras bases de datos dentro de un sistema de información bajo el control del concesionario.

Por su parte, el "control" de los registros necesita un conjunto de programas, procesos e instrucciones para almacenar, acceder, modificar y editar la información de la base de datos[48]. El control se lleva a cabo a través de un lenguaje[49] que permite determinar los privilegios de los usuarios que pueden acceder a la base de datos y los parámetros de autorización para modificar la información ahí contenida.

Desde el punto de vista de negocio, la conservación de los datos referidos en los párrafos anteriores, suele ser temporal conforme a las necesidades del negocio, por ser necesaria para atribuir el costo de los consumos realizados por el usuario de los servicios del TIC.

---

[47] Consultada el 7 de agosto de 2014, http://es.wikipedia.org/wiki/Registro_(base_de_datos)

[48] Consultada el día 7 de agosto de 2014, http://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_base_de_datos

[49] Consultado el día 7 de agosto de 2014., http://es.wikipedia.org/wiki/Lenguaje_de_Control_de_Datos

En este caso la información personal del usuario que se asocia a los metadatos para poder facturar los consumos realizados tiene un uso legítimo consistente con los fines para los cuales los usuarios proporcionan sus datos personales y los propósitos de negocio de los concesionarios.

2.3 Naturaleza comercial de los metadatos

La información del primer nivel deja registros en diversas bases de datos que permiten identificar cada comunicación. A nosotros nos interesa abordar, como lo apuntamos en el capítulo anterior, la regulación que aplica a la protección y uso legítimo de la información del primer nivel, referente a la huella de las comunicaciones, es decir, los metadatos.

Los metadatos comprenden en el caso de tráfico público conmutado de voz: El número desde el cual se realiza la llamada, el número de destino al cual la llamada es enrutada, así como, día y hora en que comenzó y terminó la comunicación. Con respecto a las comunicaciones por internet que pueden ser de voz, video o texto, también metadatos son susceptibles de registro y gestión, lo que implica el conocimiento de las direcciones IP tanto de origen y como de destino.[50] Con motivo de la asociación a la información personal del usuario con los metadatos de las comunicaciones que se realizan por una línea contratada, es posible identificar o hacer identificable al usuario final que utilizó los servicios de telecomunicaciones.

De tal suerte que, los metadatos consistentes en los registros de las comunicaciones electrónicas realizadas por una línea identificada a través de la numeración y la dirección IP, al asociarse a la información personal del usuario, adquieren la característica de datos personales, puesto que revelan información que

[50] Chris Tuppen, “Opening the Lines, A Call for Transparency from Governments and Telecommunications Companies”, Global Network Initiative, página 13, consultado el día 1 de septiembre de 2015 en https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf

identifica o hace identificable a los individuos. Por tanto, los metadatos están cobijados por el derecho a la vida privada y en consecuencia a la inviolabilidad de las comunicaciones privadas[51].

Los concesionarios están llamados a reconocer el derecho a la vida privada de los usuarios y a tratar los metadatos conforme al artículo 16 de la Constitución,

---

[51] Al respecto, es aplicable la tesis de la Primera Sala de Nuestro Máximo Tribunal con número 1ª. CLV/2011, cuyo rubro y texto señalan: DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE IDENTIFICAN LA COMUNICACIÓN. El objeto de protección constitucional del derecho a la inviolabilidad de las comunicaciones privadas, previsto en el artículo 16, párrafos decimosegundo y decimotercero, de la Constitución Política de los Estados Unidos Mexicanos, no hace referencia únicamente al proceso de comunicación, sino también a aquellos datos que identifican la comunicación. A fin de garantizar la reserva que se predica de todo proceso comunicativo privado, resulta indispensable que los datos externos de la comunicación también sean protegidos. Esto se debe a que, si bien es cierto que los datos no se refieren al contenido de la comunicación, también lo es que en muchas ocasiones ofrecen información sobre las circunstancias en que se ha producido la comunicación, afectando así, de modo directo o indirecto, la privacidad de los comunicantes. Estos datos, que han sido denominados habitualmente como "datos de tráfico de las comunicaciones", deberán ser objeto de análisis por parte del intérprete, a fin de determinar si su intercepción y conocimiento antijurídico resultan contrarios al derecho fundamental en cada caso concreto. Así, de modo ejemplificativo, el registro de los números marcados por un usuario de la red telefónica, la identidad de los comunicantes, la duración de la llamada telefónica o la identificación de una dirección de protocolo de internet (IP), llevados a cabo sin las garantías necesarias para la restricción del derecho fundamental al secreto de las comunicaciones, puede provocar su vulneración.
Amparo directo en revisión 1621/2010. 15 de junio de 2011. Cinco votos. Ponente: Arturo Zaldívar Lelo de Larrea. Secretario: Javier Mijangos y González.

por lo que **es recomendable considerar** este principio en la conservación y registro de las comunicaciones de los usuarios de conformidad con el artículo 190, fracción II de la LFTR.

2.4 Tratamiento de los metadatos por ministerio de ley

Los sistemas y redes de información de los concesionarios en México están preparados desde su creación para conservar los metadatos de las comunicaciones realizadas mediante el uso de numeración propia o en su caso, arrendada a otros socios de negocio (concesionarios), con el propósito de medir los consumos en servicio realizados por los usuarios finales y calcular el monto de la contraprestación respectiva.

En tratándose del registro y control con fines de negocio, el propósito de ese tratamiento de datos personales es consistente con la finalidad para la cual el usuario autorizó el uso de su información personal al contratar los servicios.

En este escenario, las implicaciones para la vida privada de los usuarios finales de cada concesionario, exige establecer medidas adecuadas para mitigar las amenazas que existen en el ecosistema de las TIC contra aquella y los datos personales, procurado el uso legítimo de la información personal, así como, la seguridad de la información.

En un escenario en el que el registro y control de los datos personales digitalizados, que son generados por las comunicaciones realizadas por los usuarios, se lleva a cabo en cumplimiento a lo ordenado en una ley; es natural concluir, que los principios de proporcionalidad y licitud están implícitos en las acciones que dan cumplimiento a la ley, precisamente, porque el origen del actuar de los obligados concesionarios está en la regulación. En otras palabras, están justificados en el orden público y el interés social del que está envestida la LFTR, independientemente de los derechos que se vean restringidos al cumplir con la medida regulatoria en materia de telecomunicaciones.

En este nivel de análisis, las razones de los concesionarios o autorizados para conservar la información personal de los usuarios, se consideran adecuadas a la ley. Sin embargo, la afectación potencial a los usuarios que puede presentarse

en el ecosistema de TIC, obliga a los concesionarios a profundizar en el análisis de los aspectos de privacidad y protección de datos de los usuarios, considerando los restantes principios que deben están llamados a cumplir y así los deberes que les impone la ley, mientras los metadatos estén bajo su control durante el tiempo que establezca la ley.

De esta manera, es posible advertir la proporcionalidad de la medida regulatoria impuesta a los concesionarios, respecto a la invasión en la vida privada de los usuarios, considerando la necesidad de seguridad en una sociedad. Por tanto, actuar en consecuencia de acuerdo con el eslabón que ocupan dentro de la cadena de valor de cumplimiento de la regulación atendiendo al principio de responsabilidad.

Ahora bien, cuando el registro y conservación se realiza con el propósito de colaborar con la justicia, pareciera que la finalidad del tratamiento no es consistente con el consentimiento del usuario titular de los datos personales y hasta cierto punto, quizá incompatible con la voluntad de los usuarios que contratan servicios de TIC.

Además, no olvidemos que la conservación se realiza en forma masiva de tal suerte que el tratamiento realizado por todos los concesionarios en México se vuelve más sensible, puesto que no sólo se conserva el registro de las comunicaciones realizadas por un usuario en específico sino de toda la sociedad, de modo que con las herramientas informáticas adecuadas, es posible conocer los números telefónicos a los cuales han llamado los usuarios del concesionario, así como, el día y hora en que comenzó y terminó cada comunicación en específico, por un periodo hasta de 2 años, haciendo disponible esa información respecto de todos los concesionarios en México y de todos sus usuarios[52].

[52] En lo que respecta a las comunicaciones por internet, la obligación de registro y control implica, conservar las direcciones IP de origen de cada usuario y cada una de las IP de destino relacionadas a éste, de cada uno de los sitios de internet que visita, lo que representa un esfuerzo de capacidad y procesamiento que sólo puede ser atendido con una fuerte inversión en tecnología.

Aún en el caso de que ese tratamiento sea legitimado por el artículo 190, fracción II de la LFTR, existe la amenaza de vulneración, por tanto, el principio de responsabilidad debe ser atendido en la medida de la naturaleza de la información conservada y las posibles amenazas a la misma.

2.5 Valor público derivado de la protección a la información conservada

El valor público de la medida regulatoria lo encontramos en la utilidad que la información tiene para las autoridades competentes en el cumplimiento de sus funciones sustantivas. En el caso específico, el registro y control de los datos de las telecomunicaciones que se convierte en información de inteligencia, es un elemento fundamental para averiguar la ruta que siguió una comunicación. La conclusión obtenida a partir de la información bridada por los concesionarios ayuda a las autoridades competentes en la prevención, investigación y combate contra la delincuencia y amenazas a la seguridad en nuestro país[53].

La protección de la privacidad y el uso legítimo[54] de los datos personales conservados por los concesionarios, claramente, son elementos con los cuales se asegura la utilidad de la información para las autoridades y en última instancia, el valor público de la regulación.

En efecto, al incorporar en los procesos físicos y sistemas informáticos, las medidas ad hoc de protección de la información personal y la privacidad, se favorece la protección más amplia para los usuarios de los servicios de telecomunicaciones y además, se garantiza la confidencialidad e integridad de los

[53] Considerando quinto, numeral 3, párrafo sexto del Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996. Publicado en el Diario Oficial de la Federación el 2 de diciembre de 2015.

[54] El uso legítimo deriva del cumplimiento de la ley al tratar los datos derivados de las comunicaciones que hayan realizado.

metadatos de las llamadas telefónicas, así como su disponibilidad efectiva y oportuna conforme lo soliciten las autoridades en el marco de cumplimiento a la LFTR. De esta forma, los metadatos serán entregados en forma íntegra, sin alteraciones y de acuerdo a los supuestos establecidos en Ley, como un elemento de inteligencia, relevante para la investigación, prevención y combate a los delitos.

2.6 Protección jurídica de datos personales y la privacidad en las bases de datos en empresas de TIC

Como lo apuntamos en el capítulo anterior, nuestra sociedad vive grandes cambios detonados por el hecho de que el mundo está interconectado por redes de comunicación, plataformas de software y aplicaciones con funciones específicas[55]. Estas tecnologías recolectan información personal y de negocio desde cualquier parte del mundo en la que haya dispositivos móviles y fijos conectados a una red y sistemas de información, comúnmente a través de una línea con un número y usuario identificado.

Para atender los riesgos a través de toda la cadena de valor de las TIC, sus integrantes deben identificar el eslabón que ocupan y con base en ello, diseñar un sistema de protección adecuado a su escenario, en el que se proteja la vida privada a través del uso legítimo de los datos personales informando de ello a sus titulares. No debemos perder de vista que cualquier medida debe analizarse trazando el camino que siguen los datos de las comunicaciones desde que son generados hasta que son eliminados concluido el periodo de 24 meses, considerando la manera en que deben ser entregados a las autoridades.

Las medidas garantistas de la vida privada y protección de datos elegidos, adicionales a la seguridad de la información, no deben constituir un obstáculo para la libre circulación de la información, sino medios que aseguren un uso conforme a la ley.

[55] Todas ellas conocidas como las tecnologías de la información y comunicaciones.

En un mundo interconectado en el que las tecnologías, sensores y servicios habilitados por internet (tanto públicos como privados), funcionan en forma automática recolectando datos personales, es común que el titular no pueda evitar la recolección por estar condicionada por la ley y mucho menos, el uso que conforme a la ley se le debe dar a la información personal, como sucede en el caso de la conservación de datos con propósitos de colaboración con la justicia.

Considerando lo anterior, el principio relativo al consentimiento para el tratamiento de datos personales se vuelve inaplicable. Tal como lo señala el Grupo del artículo 29[56] en su estudio sobre el internet de las cosas, este principio se erosiona, pero no por ello, los deberes y obligaciones de los responsable con relación al tratamiento de los datos personales se opacan, por el contrario, cobran mayor relevancia, especialmente en los sectores de telecomunicaciones e informático, cuyo dinamismo es una característica intrínseca y constante, no sólo desde el punto de vista tecnológico, sino desde la perspectiva regulatoria como sucede con la LFTR.

En efecto, en el caso de los concesionarios y autorizados de conformidad con la LFTR, como encargado del tratamiento tiene que respetar los principios de protección de datos personales establecidos en ley y también el deber de seguridad (administrativo, físico y técnico).

De conformidad con los artículos 6 y 7 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), los responsables en el tratamiento de datos personales quienes registran y controlan las bases de datos de los usuarios, deben observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en ese ordenamiento, cuando conserven información personal de los usuarios de una línea, con propósitos de colaboración con la justicia.

---

[56] Opinion 8/2014 on the on Recent Developments on the Internet of Things, página 7. Que fue consultada el 27 de noviembre en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Al cumplir con los principios anteriores, se tutela la expectativa razonable de privacidad que, de conformidad con los artículos citados, debe ser entendida como la confianza que deposita cualquier persona en otra, respecto a que los datos personales proporcionados serán tratados conforme a lo que acordaron las partes y considerando lo que establece la Ley.

Por otra parte, de acuerdo con el artículo 19 de la LFPDPPP, todo responsable que lleve a cabo tratamiento de datos personales (como el registro y control de datos de las comunicaciones electrónicas) debe establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Para ello, los concesionarios deben tomar en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

A partir de lo dispuesto en estos artículos, se han desarrollado una serie de disposiciones de carácter general, como los Parámetros de Autoregulación vinculantes[57], las Recomendaciones en materia de seguridad de datos personales, así como el Sistema de Gestión de Seguridad de Datos Personales[58]. Los anteriores instrumentos, son un referente que constituye un estándar de aplicación de la ley y una herramienta útil para establecer sistemas de protección de la privacidad y datos personales.

Los documentos anteriores, establecen las directrices generales en México para proteger los datos personales, durante la conservación de los mismos, mismas que están enfocadas en el cumplimiento de los alcances establecidos en la ley,

---

[57] Los cuales fueron consultados el día 2 de noviembre de 2015 en http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Parametros%20de%20Autorregulacion.pdf

[58] Los cuales fueron consultados el día 2 de noviembre de 2015 en http://inicio.ifai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf

principios para proteger la privacidad y los datos personales, así como deberes de los responsables en aspectos de seguridad. En suma, buscan la protección de estos datos y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas, de conformidad con el artículo 1 de la LFPDPPP.

Capítulo 3

Conservación y entrega de datos personales de conformidad con el artículo 190, fracción II de la LFTR

Capítulo 3: Conservación y entrega de datos personales de conformidad con el artículo 190, fracción II de la LFTR

.

3.1Análisis del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión

El artículo 190, fracción II citado, es una disposición muy controversial por las implicaciones a la privacidad y protección de datos, que la conservación y registro masivos generan. El artículo en comento establece la obligación de conservación de los datos de las comunicaciones realizadas por los usuarios, limitándola a los **"…concesionarios de telecomunicaciones y, en su caso, los autorizados…"** quienes deberán conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los metadatos de las comunicaciones de los usuarios.

El control y registro de los metadatos es obligatorio a partir de la fecha en que se haya producido la comunicación. Es una obligación para los concesionarios y autorizados que nació con la LFTR, que no está sujeta a ninguna condición previa, pues no requiere un acto de una autoridad que aplique la fracción II aludida, por el cual comience la conservación de los metadatos. Con la sola entrada en vigor de la ley u otorgamiento del título de concesión, las bases de datos de colaboración con la justicia deben ser creadas o habilitadas para entregar la información a las autoridades en forma física o lógica.

Los metadatos que sean conservados, tienen la virtud de identificar las comunicaciones realizadas por los usuarios, y consisten en:

> "…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…"

En el caso de los concesionarios de servicio fijo, conforme al artículo décimo cuarto de los Lineamientos emitidos por el IFT[59], los concesionarios deben registrar y controlar el nombre y dirección del usuario registrado, tipo de comunicación, números de origen y destino, duración, fecha y hora de la comunicación.

El periodo de conservación de los datos anteriores comprende 2 años. Los primeros 12 meses los datos personales deben conservarse en bases de datos que permitan su consulta y entrega inmediata a las autoridades competentes, a través de los medios físicos y electrónicos considerando para ello 24 horas, así como el mismo medio físico o electrónico por el que los concesionarios recibieron la solicitud[60]. Durante el segundo periodo, la entrega de la información debe realizarse

---

[59] Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996. (los Lineamientos)

[60] Conforme al artículo quinto del Acuerdo anterior *"Los Concesionarios y Autorizados deberán atender los requerimientos que se presenten por medios físicos (en papel) o por medios electrónicos y deberán responder a dicho requerimiento por el mismo medio en que los recibieron, siempre que no exista otra disposición expresa de la autoridad competente.*

En el caso de requerimientos presentados por medios electrónicos, los Concesionarios y Autorizados deberán incluir en su respuesta los archivos en formato ".pdf", ".csv", ".xls" u otros que les hayan sido indicados por las Autoridades Designadas, sin leyendas o ***claves de seguridad que impidan o limiten su utilización.***

dentro de las 48 horas siguientes. En ambos casos, el periodo se cuenta a partir de la recepción de la solicitud.

En ambos casos, los obligados a la conservación con propósitos de colaborar con la justicia deben considerar los mecanismos que determinen las autoridades competentes.

Conforme al artículo 190 de la LFTR, en relación con el diverso décimo séptimo de los Lineamientos, los concesionarios y autorizados *"son responsables respecto a la posesión, protección, tratamiento y control de los Datos Personales de los particulares*" por lo que deben cumplir con los principios de la LFPDPPP y tomar las medidas técnicas necesarias para proteger los metadatos conservados. Esto es, la LFTR prevé una salvaguarda con el fin de garantizar que en la conservación, los datos sean cuidados, protegidos, no manipulados, accedidos ilícitamente, destruidos, alterados o cancelados.

Conforme a los Lineamientos, debe existir un Área Responsable[61] de realizar la entrega de los datos conservados. La recomendación es que esta función debe ser encomendada a colaboradores específicos dentro de su estructura organizacional, quienes pueden tener acceso al manejo y control de la información personal para entregarla a las autoridades, así como al cuidado del cumplimiento del uso de los metadatos conforme a la ley, velando por su protección.

Finalmente, los Lineamientos y la LFTR establecen que se *"… prohíbe la utilización de los datos conservados tanto para fines distintos a los previstos en el*

Las Autoridades Designadas podrán acordar con los Concesionarios y Autorizados los campos que contendrán los archivos ".pdf", ".csv" o ".xls" a los que se refiere el presente lineamiento."

[61] Artículo segundo fracción I de los Lineamientos *"…área designada por los Concesionarios y Autorizados disponible las veinticuatro horas del día, los trescientos sesenta y cinco días del año, para la atención de los requerimientos de las Autoridades Designadas sobre localización geográfica en tiempo real de los equipos de comunicación móvil, entrega de datos conservados, así como intervención de comunicaciones privadas;"*

Capítulo Único del Título Octavo de la LFTR, …". Por lo que el principio de responsabilidad se cumple al tratar los metadatos sólo para propósitos de colaboración con la justicia al conservarlos por 24 meses y en su caso entregarlos previa solicitud por escrito.

3.2 Privacidad y protección de datos personales mientras se cumple con la medida regulatoria

El concepto de privacidad y protección de datos es contextual e histórico, evoluciona con los cambios tecnológicos, políticos o por el paso del tiempo, siempre en función de la sociedad en la que se estudie el fenómeno. En nuestro caso, la regulación en la materia es reciente.

Por supuesto, sí existe previsión expresa en el artículo 190, fracción II de la LFTR y los Lineamientos, que sujeta a los concesionarios a cumplir con la legislación en materia de protección de datos personales en posesión de los particulares en México. Basta leer el precepto legal para conocer los alcances generales de la salvaguarda en materia de privacidad y protección de datos personales.

La obligación anterior implica el cumplimiento de la regulación en materia de privacidad y protección de datos contenida en la LFPDPPP, con los matices y excepciones propios derivados de la finalidad que se busca alcanzar con la conservación con propósitos de colaboración con las autoridades. Atentos al valor público de los datos conservados, la protección de los datos personales y la privacidad de los usuarios, debe realizarse en forma preventiva, desde el diseño de los procesos y sistemas informáticos.

Nuestro sistema normativo no establece una disposición que sujete a los concesionarios a implementar la protección de datos personales y la privacidad en forma preventiva, desde el diseño de los sistemas de información y la creación de bases de datos que serán consultadas por las autoridades competentes.

La aplicación de los principios y el cumplimiento de los deberes en la materia, no puede iniciarse después de que la conservación de datos en las bases ad hoc, se haya materializado, porque la mayor protección para los usuarios no sólo se logra cumpliendo los aspectos correctivos, además, se tutela incorporando preventivamente la privacidad y protección de datos personales de los usuarios, desde el diseño de los sistemas informáticos o procesos físicos típicos, mediante los cuales, respectivamente, se realizará la conservación y la entrega de los metadatos de las comunicaciones vinculadas a un número telefónico por el cual los usuarios realizaron llamadas.

Como se dijo, las bases de datos prexistentes en los sistemas informáticos de los concesionarios fueron creadas con fines estrictamente de negocio. Naturalmente, son la fuente de la que se extraerán los datos de las comunicaciones así como los datos de los usuarios que las realizaron, que alimentarán otra u otras bases de datos creadas con el propósito exclusivo de conservar la información y permitir su entrega requerida por las autoridades de seguridad y procuración de justicia, ya sea en forma física y/o electrónica.

Los datos que alimentan de las bases de datos de negocio, con el propósito de realizar las actividades de conservación (registro y control de los datos de las comunicaciones realizadas), así como para entregar esa información con herramientas informáticas o simplemente continuar con los medios físicos de entrega típicos, tendría que considerar las recomendaciones de privacidad por diseño anteriores. Estos conceptos deben ser considerados en la construcción misma de la solución de software y hardware o el medio ad hoc elegido para cumplir con la conservación y entrega.

Es conveniente que los concesionarios observen constantemente el cumplimiento a las disposiciones y recomendaciones en materia de protección de datos y privacidad, procurando que el sistema y los procesos creados al efecto, siempre atiendan la expectativa razonable de privacidad de los usuarios[62] evitando

[62] Que de acuerdo al artículo 6 de la Ley Federal de Protección de Datos Personales, consiste en la confianza que deposita el usuario en los concesionarios, respecto de

la revelación y sólo por excepción, ante un requerimiento de información de autoridad competente, sea posible modificar ese estado al realizar la entrega. En consecuencia, se entregue la información sólo a la autoridad competente con independencia de la voluntad del usuario.

Cada sistema preexistente o que sea creado para cumplir con la medida regulatoria tendrá su diseño particular, su estructura propia, la cual estará alineada con los recursos técnicos y humanos del concesionario, así como, al propósito de la medida regulatoria -entregar la información requerida por las autoridades en forma efectiva y oportuna- sin comprometer la privacidad y el debido tratamiento de la información personal.

Es recomendable que el concesionario realice un diagnóstico enfocado en la privacidad y protección de datos personales respecto del sistema preexistente (que tiene un propósito de negocio) y en el caso de la creación de uno nuevo, para cumplir con la regulación de colaboración con la justicia, incorporar estos conceptos desde el diseño del sistema (considerando un propósito de orden público). En ambos casos, lo primero que se debe hacer es inventariar los datos personales y después identificar la cadena de valor de éstos.

Así, desde el diseño de la solución e implementación de los medios de entrega físicos, podremos conocer el camino que seguirán los datos por toda la cadena de valor, desde que son recolectados, conservados, entregados y hasta que son eventualmente eliminados del sistema creado por el concesionario. Este análisis es indispensable para medir el grado de exposición a riesgos de los datos personales en cada eslabón de la cadena, en función de las medidas establecidas contra las amenazas que pudieran presentarse.

---

que los datos personales consistentes en los metadatos de sus llamadas, serán tratados conforme a lo que acordaron las partes en los términos establecidos por la esta ley y la LFTR. La expectativa razonable de privacidad debe ser considerar dúctil, con independencia de la voluntad del usuario. A esfera que comprende dicha expectativa se ve reducida con motivo de una razón de orden e interés públicos.

3.3 Cumplimiento a los principios de protección de los datos personales conservados para la colaboración con las autoridades

En principio, debe quedar claro que el concesionario es el responsable en términos de la LFPDPPP, frente a los usuarios, con todas sus consecuencias, por el tratamiento consistente en el registro y control en sus sistemas informáticos, así como por la entrega de datos a las autoridades que emitan los requerimientos de información derivados del artículo 190, fracción II de la LFTR citado[63].

En este punto, es relevante señalar que el tratamiento de la información personal, se llevará a cabo, por una excepción de la ley, con independencia del **consentimiento** del usuario, siendo **lícita** la conservación por ser de orden público. La LFTR señala que los datos conservados no pueden ser utilizados para otra **finalidad** que no sea la de colaboración con las autoridades, esta es una prohibición expresa que claramente puede generar responsabilidad a los concesionarios en caso de incumplimiento por faltar al principio de **lealtad**[64].

Por la importancia y nivel de riesgo que para la privacidad y protección de datos de los usuarios supone el cumplimiento de la medida regulatoria establecida en la LFTR, **es recomendable** que el concesionario **informe** a éstos[65] -a través de una medida compensatoria- que en cumplimiento a la regulación en materia de telecomunicaciones, está obligado a conservar los registros de las comunicaciones hechas por la línea contratada durante el periodo de 24 meses. Además, que previo

---

[63] Recordemos que el artículo en comento no establece expresamente obligaciones atribuibles a las autoridades pertenecientes al sector público, que hagan extensiva la responsabilidad por el uso de los datos personales conservados tanto a concesionarios como a las autoridades. No existe un principio de continuidad expresamente plasmado en la LFTR que prolongue la protección de la información personal en ambos sectores.

[64] Artículo 190, fracción II, segundo párrafo de la LFTR.

[65] De conformidad con el artículo 16 de la LPDPPP. Las excepciones se presentarán en el ejercicio de los derechos ARCO.

requerimiento debidamente fundado y motivado, hecho por las autoridades previstas en el artículo 189 de la LFTR, el Concesionario entregará en forma eficiente y oportuna la información conservada que le sea requerida de conformidad con la ley y con los Lineamientos que al efecto expidió el Instituto Federal de Telecomunicaciones[66].

Como parte de las acciones convenientes en un entorno de protección a la privacidad y datos personales en el sector de telecomunicaciones, el concesionario debe realizar su inventario de datos personales de las comunicaciones de los usuarios y el diagrama de la cadena de valor -el proceso- para la colaboración con la justicia, ya que son herramientas indispensables en la planeación previa a destinar recursos económicos y humanos para cumplir con la regulación.

Son dos herramientas útiles que ayudarán a definir los alcances de la regulación de protección de datos y de colaboración de la justicia, considerando **la finalidad** de la conservación de los registros de las comunicaciones en bases de datos personales generados por las comunicaciones de los usuarios de los servicios de telecomunicaciones, con propósitos de colaboración con la justicia.

Derivado de su calidad de responsable, el concesionario de que se trate tiene la obligación de cumplir con los principios de protección de datos personales y respetar la expectativa razonable de privacidad de sus usuarios, considerando las excepciones que la propia ley establece[67]. Asimismo, garantizar el ejercicio de los

---

[66] ACUERDO mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996. Publicado en el Diario Oficial de la Federación el día 2 de diciembre de 2015, consultado el día 21 de diciembre del mismo año en http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

[67] Por ejemplo, tratándose del principio del consentimiento, no es necesario obtenerlo del usuario para realizar la conservación, registro, control y entrega de datos personales a las autoridades, de conformidad con el artículo 10, fracción I de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

derechos de acceso, rectificación, cancelación y oposición, salvo que exista una excepción legal.

Para el derecho a cancelar los datos, habrá que observar el transcurso del plazo de 24 meses que dura la conservación, o en el caso de acceso solicitado por un usuario, la orden expresa de la autoridad por la que se prohíba revelar a los usuarios los datos personales conservados o que han sido entregados a la autoridad con motivo de un requerimiento o la prohibición de borrado, por existir un proceso jurisdiccional y finalmente, la limitación al derecho de oponerse a la entrega de los metadatos a las autoridades[68].

El cumplimiento de la regulación de datos personales y privacidad, le exige a los concesionarios establecer medidas físicas, técnicas y administrativas que garanticen la integridad y la seguridad de los datos personales con base en estándares internacionales[69]. Al respecto, el SGSDP es una herramienta idónea para disminuir la exposición de los activos de información[70], considerando el valor de los activos y la posibilidad de disociación[71] de los datos personales respecto de

---

[68] De conformidad con el artículo 34, fracción IV de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[69] Ob Cit (66). Los estándares internacionales pueden ser: ISO/IEC 27001 Information technology -

Security techniques - Information security management systems - Requirements y/ o NIST Special Publication 800-

53Security and Privacy Controls for Federal Information Systems and Organization

[70] Conforme el número de personas que acceden a estos mediante controles administrativos, técnicos o físicos.

[71] Los artículos 3, fracción VIII y 10, fracción III de la LFDPPP, establecen que la disociación es el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo. Derivado de ello, cuando los concesionarios realizan la disociación de datos personales, es aplicable otra excepción al consentimiento, porque no se requeriría el consentimiento.

sus titulares[72].

Por ejemplo, si existen varias bases de datos en los sistemas de información del concesionario, que no precisamente fueron creadas con motivo de la regulación de seguridad y justicia, pero que al combinar sus activos de información, permitirían asociar la información personal a los metadatos de las comunicaciones electrónicas con el objeto de colaborar con las autoridades de seguridad y justicia, dichas técnicas para anonimizar los datos personales como una medida adicional, pueden ser muy útiles para el concesionario en la protección de datos personales.

El SGSDP de la mano con el modelado de la cadena de valor, también permiten documentar lo que se va a hacer con los datos y quiénes tienen acceso a éstos, con el objeto de evitar el uso, acceso o tratamiento no autorizados; el daño, alteración o modificación no autorizada y el robo, copia, pérdida o destrucción de los datos personales[73].

Por lo que se refiere al control del uso, divulgación, obtención, almacenamiento, cancelación o bloqueo de los datos conservados, este SGSDP también brinda elementos para identificar las medidas de seguridad[74], para documentar en un manual la forma en que se cumplirá con los requisitos de la LFTR, consistentes en establecer el control y registro sobre las bases de datos.

---

[72] En el caso, es conveniente aplicar técnicas para anonimizar los datos personales derivados de las comunicaciones realizadas por los usuarios. Al respecto, el grupo del artículo 29 ha emitido criterios referentes a técnicas para anonimizar los datos personales. Consultado el 27 de diciembre de 2015 en http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf

[73] Artículo 63 del Reglamento de la LFPDPPP.

[74] Al respecto, los artículos 61 y 62 del Reglamento de Protección de datos establecen los factores y acciones vinculados a las medidas de seguridad, de modo que es necesario que los Concesionarios consulten este marco de referencia para establecer las medidas adecuadas para controlar y registrar los datos conservados.

Al respecto, una metodología adecuada para lograrlo lo anterior, es el análisis de brecha[75] de los sistemas informáticos prexistentes de negocio, cuyos resultados sean considerados por los colaboradores del concesionario en el diseño del sistema de registro y control para conservar los metadatos de las comunicaciones y en los medios físicos o lógicos previstos para entregarlos a las autoridades. El Área responsable debe realizar este estudio en forma periódica con el fin de actualizar el nivel de protección a la privacidad y datos personales almacenados, tanto en las bases de datos de negocio como en las de conservación con propósitos de colaboración con la justicia. El análisis de brecha es cíclico, fundamental para identificar en forma dinámica los riesgos para los datos personales conservados y las medidas de protección más adecuadas de conformidad con la ley.

3.4 Prácticas regulatorias de seguridad contra riesgos de las bases de datos para la colaboración con la justicia

Si bien el tratamiento de los metadatos está definido por la LFTR, así como por los Lineamientos**, el principio de responsabilidad** corresponde cumplirlo a los concesionarios. Este principio se atiende estableciendo a la interior de la organización las medidas regulatorias adecuadas a la sensibilidad de los datos personales. **Es recomendable** que estas medidas comprendan por una parte el cumplimiento a lo establecido en la ley y por la otra, a las buenas prácticas.

A este respecto, el artículo 60 del Reglamento de la LFPDPPP, establece que, para determinar las medias de seguridad, es necesario considerar el riesgo inherente al dato personal en específico, su sensibilidad, el desarrollo tecnológico y las posibles consecuencias de una vulneración para los titulares. Adicionalmente,

[75] Este estudio se basa en las medidas de seguridad existentes para proteger los datos personales y aquellas que falta implementar para elevar el nivel de protección de datos personales. Es un estudio que nos dice en dónde estamos en términos de seguridad y a dónde queremos llegar. Ver artículo 61, fracción V del Reglamento de la LFPDPPP.

este precepto establece que el responsable procurará tomar en cuenta el número de titulares, vulnerabilidades previas, el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para terceros.

Por su parte, los Lineamientos señalan que los concesionarios y autorizados serán responsables de que los protocolos utilizados para la adquisición, desarrollo y/o implementación de las Plataformas Electrónicas, garanticen la integridad y seguridad de la información transmitida, manejada y resguardada, y funcionen con base en estándares internacionales relacionados con la salvaguarda y protección de los datos personales de los usuarios, así como para la cancelación y supresión segura de la información, tales como*: ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements y/o NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*[76].

En ese sentido, el concepto de seguridad de la información comúnmente aceptado[77], que también es aplicable a la protección de datos, consiste en considerar que cualquier sistema, sean físicos o informáticos contemplen los siguientes requerimientos.

I. ***Confidencialidad.*** *La información debe estar disponible sólo para los usuarios autorizados y además, tener controles que la protejan contra el acceso no autorizado a los sistemas y redes de información.*
    - ***Control de acceso.*** *Se otorga mediante la autenticación adaptándolo al rol que tiene la entidad o persona en el sistema.*

II. ***Integridad.*** *Consiste en las garantías que aseguren la exactitud y la calidad de la información, así como los sistemas para detectar cualquier modificación a la información. También refiere a los métodos de procesamiento para evitar*

[76] Artículo octavo, fracción V de los Lineamientos.

[77] ISO/IEC 27002:2005, Information Technology – Security techniques – Code of practice for security management. Citado por Kamruzzaman, Joarder et. al. “Security and Privacy in RFID Systems”, IGI Global Retrieved from www.knovel.com.

la modificación no autorizada de la información, mientras se accede a ella o mientras es enviada.

III. ***Disponibilidad.*** *Permite que los usuarios autorizados, en el momento que se requiere, accedan ágilmente a la información y los activos de negocio asociados. El sistema debe atender las solicitudes de consulta, cuando sea requerido.*

IV. ***Autenticación.*** *Consisten en asegurar que la entidad o la persona física que pretende acceder a la información, es quien dice ser. La autenticación es un control de acceso que debe realizarse cuando se establece la comunicación y mantenerse durante el tiempo que dura la comunicación entre las puntas (equipos generadores de contenido y receptores de la información).*

V. ***No repudio.*** *Una entidad o persona autenticada que participó en la comunicación después no podría negar su participación y haber accedido a la información.*

Los requerimientos anteriores se interrelacionan complementándose unos a otros. Además, son transversales a los sistemas y redes de información, que alimentan las bases de datos y claramente aplicables en las acciones que tomen los concesionarios en la conservación de los datos generados por las comunicaciones de los usuarios, así como para el proceso de entrega de los metadatos a las autoridades en forma oportuna.

En el caso de esta investigación, nos referimos a las bases de datos que contienen los registros de las comunicaciones electrónicas hechas a través de una línea otorgada por los concesionarios o en su caso, arrendada. En este escenario, las medidas deben ser establecidas considerando los principios anteriores, con el fin de reducir los riesgos típicos y atípicos para las bases de datos en los sistemas y redes de información destinadas a la conservación con propósitos de colaborar con la justicia.

El riesgo es la posibilidad de que una amenaza se materialice aprovechando una vulnerabilidad de los sistemas de información o, dicho de otra manera, la probabilidad de que ocurra un incidente que cause un impacto con un determinado

daño en los sistemas de información, en las bases de datos de que se trate. Estos riesgos son de dos tipos, mismos que describimos a continuación[78]:

- ***Para las personas:*** *Se concreta en la pérdida de información la utilización ilícita o fraudulenta de los datos y sus consecuencias.*
- ***Para las organizaciones:*** *Son más variados con la percepción de falta de respeto a la privacidad de las personas; la aparición o el incremento de los costos de rediseño del sistema informático; la pérdida de reputación e imagen pública y, la posibilidad de acciones de investigación y sanción por parte de la autoridad de protección de datos.*

El artículo 63 del Reglamento de la LFPDPPP, establece un catálogo que podemos referir como una fuente para identificar los riesgos comunes que pueden culminar en una vulneración a las bases de datos de colaboración con la justicia. En términos generales, esta disposición establece, que la protección de datos personales debe enfocarse contra el daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.[79]

El entonces órgano regulador[80] en materia de protección de datos, en su Recomendación General en materia de protección de datos personales, señaló que la adopción de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), es necesaria para la

---

[78] Guía para una evaluación de impacto en la protección de datos personales 2014 de la Agencia Española de Protección de datos personales, consultada el día 15 de noviembre de 2015 en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

[79] Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, INAI,
Noviembre 2014, página 2, consultado el día 15 de noviembre de 2015 en http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementaci%C3%B3n_SGSDP_ene2014.pdf

[80] Instituto Federal de Acceso a la Información y Protección de Datos.

seguridad de datos personales[81]. Este sistema cobra relevancia para la protección de datos personales de los usuarios de comunicaciones realizadas por una línea, cuyos metadatos son conservados con propósitos de colaboración con la justicia.

Con motivo el SGSDP, el INAI emitió la Guía[82] que contempla diversas definiciones, entre ellas, la definición de **riesgo** que lo conceptualizamos como un binomio constituido por la probabilidad de que un incidente ocurra y la idoneidad de las medias establecidas para evitar tanto el incidente como sus consecuencias desfavorables. Dicho **incidente es** una circunstancia en la que una amenaza explota una vulnerabilidad.

I. ***La amenaza es*** *un evento con capacidad de causar un daño a la persona o a la organización.*

II. ***Una vulnerabilidad es*** *la ausencia o debilidad de seguridad en la información que puede ser explotada por una amenaza.*

Al conocer el riesgo, es posible **evaluar cómo reducir la probabilidad de que ocurra, así como conocer el impacto** que un incidente de vulneración podría tener en los datos personales conservados en colaboración con la justicia.

Con este conocimiento se facilita identificar las medidas de seguridad adecuadas para cumplir con la confidencialidad, disponibilidad e integridad de la información personal.

Se recomienda seguir los pasos de la Guía para la implementación de un Sistema de Gestión de la Seguridad de los Datos Personales publicada por la autoridad reguladora en México[83], contiene el proceso de gestión de la seguridad de la información.

---

[81] RECOMENDACIONES en materia de seguridad de datos personales. Publicadas en el Diario Oficial de la Federación el día 30 de octubre de 2013.

[82] Ob. Cit (13). Este es el documento al que nos referimos, del que se obtuvieron todas las definiciones que se exponen a continuación.

[83] Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos.

En el siguiente cuadro podemos advertir claramente el modelo denominado “Planificar-Hacer-Verificar-Actuar” (PHVA), para el proceso de gestión en comento.[84]

Fase del PHVA	Actividades
Planificar	Se identifican políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por la organización (meta).
Hacer	Se implementan y operan las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
Verificar	Se evalúan y miden los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.
Actuar	Se adoptan medidas correctivas y preventivas, en función de los resultados y de la revisión, o de otras informaciones relevantes, para lograr la mejora continua.

Cuadro 1. Fases y actividades del PHVA

Fuente: Parámetros de Autorregulación en materia de Protección de Datos Personales.

Como se menciona en dicha Guía, el modelo de la figura anterior, tiene como objetivo proveer un marco que nos permite dirigir y controlar el tratamiento de datos personales generados por las comunicaciones electrónicas y al mismo tiempo, mantener vigente y mejorar la protección de los datos de los usuario y los metadatos que los identifican, que son conservados para el cumplimiento de la LFTR, incorporando las buenas prácticas de seguridad en la conservación.[85] Es un modelo dinámico cuyo producto final, normalmente, es el insumo inicial para correr nuevamente el modelo, con la finalidad de mejorar la gestión, perfeccionándola con cada ejecución de la herramienta.

En un mundo interconectado, las amenazas externas para las bases de datos de los sistemas y redes de información de los concesionarios crecen en forma

[84] Ob. Cit 12, página 8

[85] Ob. Cit (78), página 9.

exponencial en función del número de los eventos de comunicaciones y amenazas que pueden presentarse, desde cualquier parte del mundo.

En particular, aquellas bases en las que se controlan y registran los datos de las comunicaciones electrónicas realizadas por los usuarios de una línea, deben ser resguardadas considerando la privacidad y protección de datos personales, aplicando medidas que respondan a los riesgos de fuentes remotas. Sin duda, los aspectos internos organizacionales para la protección, también son fundamentales, aunque, obedecen a escenarios en los que existe mayor capacidad de control de los riesgos y de los colaboradores como conductores de riesgos.

En ese sentido, la regulación que impone la obligación de conservación de los metadatos de las comunicaciones, al ordenar la concentración de información en los sistemas de información del concesionarios, genera un conductor de riesgos internos y externos para la privacidad y la información personal de los usuarios de estos servicios, ya que la información contenida en las bases de datos que deben ser creadas, constituye un activo[86] atractivo para el análisis lícito o ilícito que puede ser realizado por terceros (sectores público o privado) utilizando herramientas tecnológicas muy avanzadas (analytics).

El resultado derivado del análisis de la información personal contenida en esas bases de datos, desde el punto de vista del sector público puede ayudar a satisfacer necesidades de la colectividad (seguridad, salud, etc). En ambos casos, la sola conservación genera el activo y los riesgos asociados a este, por ello, las medidas deben ser implementadas desde la recolección, durante la conservación-entrega y finalmente, al cancelar dichos datos.

[86] Ob. Cit (79), página 6. “Activo. La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.”

3.5 Inventario y clasificación de los datos de las comunicaciones

El inventario de los datos personales para la colaboración con la justicia, es el primer paso en la protección de la privacidad y datos personales de los usuarios de una línea telefónica. Sin un inventario de los datos personales desconoceríamos el activo de información objeto de la tutela y por ende, estaríamos impedidos para identificar las medidas más adecuadas para reducir los riesgos asociados a éstos por su valor.

La fuente regulatoria que nos ayude a identificar los metadatos que deben ser conservados, es el artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión, por lo tanto, la descripción del contenido en ese precepto tiene que ser considerada al hacer el registro para inventario. Además de esta fuente, en la regulación emitida por el IFT se estableció que el registro de comunicaciones se llevaría sólo respecto de los recursos del Plan Técnico Fundamental de Numeración, es decir, sólo de líneas telefónicas con numeración asignada a los concesionarios y sus llamadas, excluyendo por el momento los registros de comunicaciones de acceso a internet.

En adición al listado previsto en la norma, **se recomienda** invocar una fuente real. En ese sentido, los datos personales de las comunicaciones realizadas por los usuarios que son efectivamente conservados con propósitos de negocio y los datos que las autoridades de seguridad y justicia, realmente solicitan en el ejercicio de sus actividades sustantivas, son fuentes reales de los datos que pueden ser conservados por los concesionarios para ser entregados a las autoridades.

3.6 Regulación ejecutada en la cadena de valor para la conservación de datos destinados a la colaboración con la justicia

Tomaremos como referencia un diagrama que ejemplifique gráficamente la cadena de valor. El modelo del sistema de negocio de McKinsey[87] es una herramienta útil para este fin[88].

En efecto, si identificamos las etapas (eslabones) generales más importantes de un sistema para la colaboración con la justicia para los concesionarios y las establecemos en un orden secuencial, facilitaremos la descripción de las decisiones principales de protección con el objeto de mantener la calidad de la información y en consecuencia su utilidad para las autoridades, al mismo tiempo que se protege la privacidad y datos personales de los usuarios.

La cadena de valor es una herramienta que ayuda a identificar las medidas de protección a la privacidad y datos personales considerando cada eslabón, con lo cual se fortalece la calidad en la conservación, registro y control de los datos generados por las comunicaciones de los usuarios, así como la entrega eficaz y oportuna a las autoridades. Además, la cadena de valor nos ayudará a conocer el flujo de los datos personales desde que son recabados, procesados y hasta ser

---

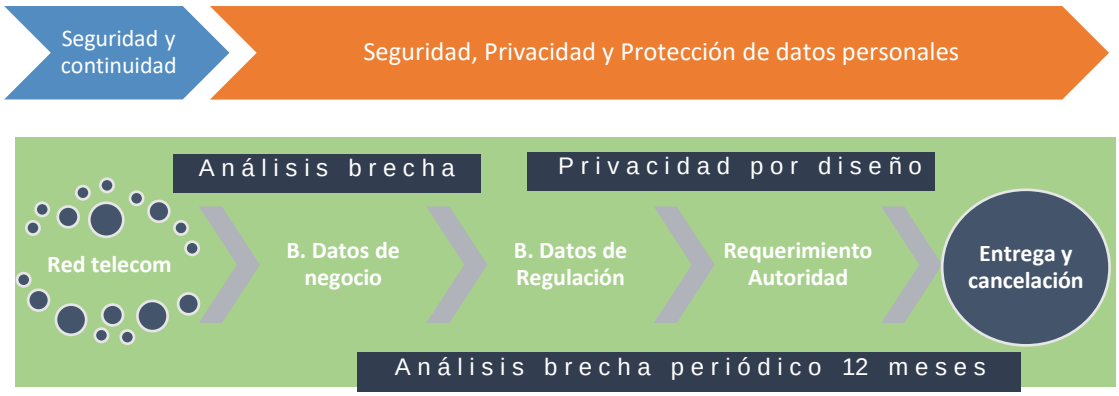
[87] The Business System, El modelo fue consultado el día 27 de diciembre de 2015 en la siguiente liga http://www.mckinsey.com/spContent/Enduring%20IdeasV2/index.html#2513607397001?sid={12533493-15A2-4A46-8359-79C823E25C73}&pid={4386CABC-8926-43B7-B922-05933D401051}

[88] Aunque este sistema típicamente está diseñado para desarrollar e identificar en cualquier organización una ventaja competitiva en el mercado (estrictamente desde el punto de vista de negocio), el concepto de dar una estructura secuencial al sistema (cadena) que da valor agregado al producto o servicio en una organización, es aplicable a nuestro caso.

cancelados (eliminados) concluido el periodo de conservación, con independencia de que hayan sido objeto de algún requerimiento de autoridad.

El sistema de colaboración puede ser representado en las siguientes capas:

Regulación aplicable a cada eslabón de la cadena de valor para colaborar



Propósitos de cada eslabón de la cadena de valor

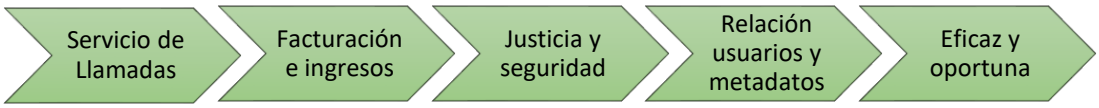


Figura 2. Cadena de valor sistema de colaboración

Fuente: Elaboración propia con base en artículo 190, fracción II LFTR.

La figura anterior nos muestra la cadena de valor del proceso de colaboración con la justicia y la regulación en materia de protección de datos personales, así como el propósito que cumple cada eslabón hasta que dicha información sea cancelada.

En primer término, en la cadena de valor observamos la red de telecomunicaciones[89] que contiene la infraestructura activa[90] integrada por los equipos que almacenan y procesan la información generada durante la prestación del servicio de llamadas contratado por el usuario[91].

En este eslabón primordialmente los aspectos de regulación están enfocados en dar continuidad a la operación de la red de telecomunicaciones, para asegurar la viabilidad del negocio y la prestación de los servicios de telecomunicaciones de que se trate, los cuales son considerados servicios públicos de interés general[92] .

Los equipos citados contienen las bases de datos de negocio, utilizadas con la finalidad de generar las facturas correspondientes a los consumos realizados por los usuarios y obtener ingresos de ellos. En este eslabón encontramos la

---

[89] De acuerdo con el artículo 3, fracción LVII, de la LFTR, la Red de telecomunicaciones es un Sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario.

[90] En el artículo 3, fracción XXVI de la LFTR, encontramos el concepto de Infraestructura activa, la cual se integra por los elementos de las redes de telecomunicaciones que almacenan, emiten, procesan, reciben o transmiten escritos, imágenes, sonidos, señales, signos o información de cualquier naturaleza.

[91] Desde la perspectiva de la inviolabilidad del contenido de las comunicaciones, las cuestiones de privacidad podrían invocarse en este eslabón como parte de los aspectos regulatorios que le son aplicables a los concesionarios de las redes de telecomunicaciones, sin embargo, el nivel de contenido de las llamadas telefónicas, escapa a la medida regulatoria de conservación de datos que abordamos en este trabajo, cuyo objeto está enfocado en un nivel previo, referente a los metadatos que identifican sólo las comunicaciones de los usuarios, no traspasan hasta el contenido de éstas.

[92] De conformidad con el artículo 6, apartado B, fracción II de la Constitución.

información de los usuarios regulada por la LFPDDPP y su reglamento, no sujeta estrictamente al propósito de colaboración con la justicia, cuya finalidad atiende a cuestiones de negocio, con impactos en los derechos del consumidor y protección de la información personal. Aunque la protección de la información personal de estas bases de datos es regulada por las disposiciones de protección de datos personales su propósito, al final, es de negocio, no le es aplicable el artículo 190, fracción II de la LFTR, ni las consecuencias de este precepto que obliga a la conservación y entrega de información personal a las autoridades con un propósito de orden e interés públicos. Por otra parte, el propósito de las bases de datos destinadas a cumplir con la regulación en materia de telecomunicaciones para colaboración con las autoridades de seguridad y justicia, no es privado, sino de orden e interés públicos. Mediante el uso de la información generada en las bases de datos de negocio del concesionario, se crea el insumo que alimenta las bases de datos creadas con propósitos de colaboración para aquellas autoridades que soliciten la información. Considerando esa dualidad constituida por las fuentes de información del sector privado, para satisfacer ciertos fines de orden e interés públicos, presentamos una secuencia de pasos en el inciso (a) de la cadena de valor (figura siguiente).

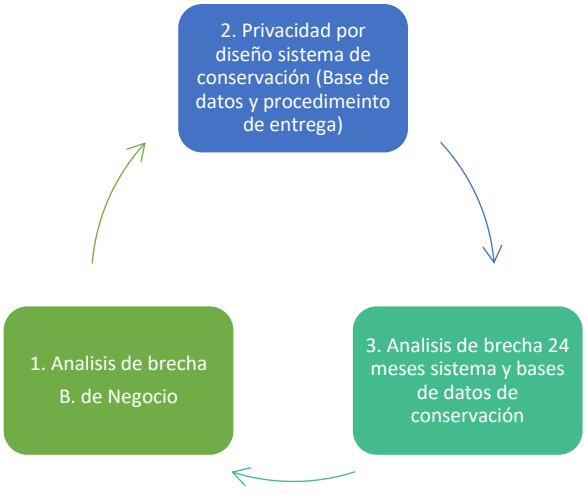


Figura 3. Ciclo de mejora continua

Fuente: Elaboración propia con base en artículo 190, fracción II LFTR.

El “Análisis de brecha” es el primer paso de un estudio de regulación de conformidad con LFPDPPP, que se aplica al sistema para generar las bases de datos de negocio preexistentes en la infraestructura del concesionario.

El segundo paso, es aplicar la metodología de “Privacidad por diseño” antes de la creación del sistema para conservar los metadatos y el proceso de entrega a las autoridades, y finalmente, el aspecto cíclico en la revisión que consiste en el “Análisis de brecha periódico cada 12 meses” a todo el sistema utilizado para crear las bases de datos de regulación y el proceso de entrega.

Con esta metodología las medidas de protección a la privacidad y datos personales de las bases de datos de regulación, serán enriquecidas periódicamente. Con la experiencia obtenida, los colaboradores de los concesionarios deben hacer el diseño de los controles para acceder a la información personal y a las bases de datos que registrarán y controlarán los metadatos, así como el diseño del proceso físico o lógico de entrega de la información, contemplando las medias preexistentes y los resultados del análisis de brecha que enriquezca la protección para los usuarios y aseguren la utilidad pública de la información para las autoridades. En cualquier caso, el propósito de cada eslabón debe gobernar las medidas de privacidad y protección de datos, con el fin de no impedir el flujo de éstos desde su registro, hasta su entrega efectiva y oportuna a las autoridades.

La cadena de valor nace y concluye dentro de la organización del concesionario[93]. En la figura anterior, apreciamos que fue modelada considerando las etapas generales más relevantes del sistema que es activado permanentemente por el concesionario, para generar el activo de información (metadatos) y conservarlo por su valor público conforme a la LFTR, para que eventualmente será entregado a las autoridades hasta con una antigüedad de 24 meses.

[93] No es el propósito de este trabajo abordar aspectos referentes a las medidas que deben tomarse por parte de las autoridades de seguridad y justicia, para proteger la privacidad y el tratamiento legítimo de la información personal.

Posteriormente a ese plazo los datos deben ser eliminados cesando su conservación con propósitos de colaboración con la justicia, sin perjuicio de que las bases de datos preexistentes a la regulación permanezcan, puesto que fueron creadas con propósitos de negocio. **Es recomendable** que la cancelación de los datos personales de los usuarios (registros de comunicaciones para colaboración con la justicia) sea respaldada con una constancia que acredite su eliminación y el cese de la conservación.

Las actividades de apoyo para la cadena de valor, pueden ser realizadas por terceros que son considerados integradores en el sistema de conservación o por las áreas de la empresa que contribuyen a lograr el propósito de cada eslabón. En todos los casos los colaboradores de la organización (internos o externos) que intervengan en las actividades de apoyo, tendrán que tener claramente definido su papel y las implicaciones que su participación tengan en el nivel de exposición de los datos personales.

Una de las principales actividades de apoyo de los concesionarios para cumplir con los extremos del artículo 190, fracción II, son los centros de datos para almacenar los datos personales. **Es recomendable** que tanto en el caso de que el concesionario cuente con su propio centro de datos o contrate el servicio con un tercero, los datos personales deberán permanecer en el territorio nacional y hacer constar en el SGSDP y en los acuerdos respectivos que se comprometen a cumplir los principios y deberes establecidos en la ley y expresamente, que se comprometen a no conceder acceso a cualquier agencia de un tercer país que lo solicite. Las bases de datos no pueden estar fuera del territorio nacional, ni ser objeto de consulta directa por autoridades extranjeras de seguridad y justicia.

La conservación se integra por (i) el registro de los datos y (ii) el control que de las bases de los mismos se tiene. Mediante el "registro" de los datos de las comunicaciones realizadas por los usuarios, los concesionarios le dan un orden lógico a éstos de manera que sean susceptibles de consulta con propósitos de colaboración con las autoridades; y a través del "control" se establecen los privilegios al interior de la organización del concesionario, para conceder el acceso a la base de datos y en su caso su edición, en otras palabras, las medidas para

mantener la integridad, disponibilidad y confidencialidad de los metadatos conservados.

Además, conforme el artículo 189 de la LFTR, los concesionarios de telecomunicaciones y Autorizados están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes. Por tanto, podemos considerar que el deber de "control" de los concesionarios también conlleva la responsabilidad de asegurarse, mediante la consulta a la ley y otras disposiciones aplicables, que el requerimiento de información provenga de una autoridad facultada y que la entrega de los metadatos requeridos se apegue a lo previsto en el artículo 190, fracción II de la LFTR, estableciendo las medidas para evitar entregar a las autoridades, cualquier información personal en poder del Concesionario, que no esté prevista en la fracción en comento o en los Lineamientos.

Los mecanismos de solicitud y de entrega deben ser considerados para efectos de establecer las medidas de protección de privacidad y datos personales, que al mismo tiempo tienen como objetivo lograr la entrega efectiva y oportuna a las autoridades competentes conforme los mecanismos de solicitud y entrega de información.

3.7 Plan para proteger los datos personales en el sistema de conservación y entrega

Las recomendaciones de este trabajo, no se extienden a los aspectos tecnológicos de la prestación del servicio de telefonía que definirían los límites de la responsabilidad de conservación de los metadatos, cuando el servicio de telefonía es otorgado por más de una empresa de tecnología, en este caso de telecomunicaciones, a través de la prestación de servicios intermedios como el de interconexión de redes de telecomunicaciones[94].

[94] Artículo 3, fracción XXX de la LFTR "Interconexión: Conexión física o virtual, lógica y funcional entre redes públicas de telecomunicaciones que permite la conducción de tráfico entre dichas redes y/o entre servicios de telecomunicaciones prestados a

Todas las medidas derivadas del análisis de brecha sobre las bases de datos de negocio, la metodología de privacidad por diseño, así como el análisis de brecha periódico que se realice al sistema de conservación y entrega de datos personales con propósitos de colaboración con la justicia, deben estar contenidas en un Plan de instrumentación y seguimiento. Este manual debe contener los aspectos generales metodológicos del Sistema de Gestión de la Seguridad de Datos Personales del que se desprendan los resultados de los análisis de brecha mencionados en el párrafo anterior, así como los aspectos de privacidad y protección de datos personales desde el diseño del sistema del Concesionario.

El plan para implementar el sistema de conservación y entrega, sólo abarcaría los límites definidos por la cadena de valor del Concesionario para dar cumplimiento a la regulación, sin contemplar la conservación que pudieran realizar los revendedores u otros Concesionarios que participen en la prestación del servicio de telefonía a través de servicios intermedios.

Este plan, además, debe contemplar aspectos de transparencia[95] en los que se indique a los usuarios de servicios de telefonía, (i) cuáles son los metadatos que conservará en cumplimiento a la regulación, (ii) el hecho de que la conservación se realizará por cada comunicación realizada por el usuario y (iii) que la conservación se realizará con el propósito de colaborar con la justicia. En cuanto a las medidas tomadas para proteger la información personal y la privacidad de los usuarios, el concesionario debe comunicar a sus usuarios, la (i) existencia del Plan elaborado por el concesionario para proteger de manera razonable, los datos personales y

---

través de las mismas, de manera que los usuarios de una de las redes públicas de telecomunicaciones puedan conectarse e intercambiar tráfico con los usuarios de otra red pública de telecomunicaciones y viceversa, o bien permite a los usuarios de una red pública de telecomunicaciones la utilización de servicios de telecomunicaciones provistos por o a través de otra red pública de telecomunicaciones."

[95] Australian Government. Attorney-General´s Department. Data Retention, Frequently Asked Questions for Industry. Version 1.1 July 2015, páginas 35 y 36

privacidad de sus usuarios, (ii) las autoridades a quienes debe entrega la información personal y el sitio de internet de estas para realizar cualquier consulta u ejercicio de sus derechos.

Conclusiones

Conclusiones

1. La información personal y de negocio en las organizaciones, está rápidamente migrando de un formato analógico a un formato digital, mediante el uso cada vez más intenso de las TIC en nuestra sociedad.

2. Las TIC incrementan la velocidad con la que nos comunicamos y compartimos información, pues permiten conservar y transmitir los datos a cualquier parte del mundo en donde exista una conexión a las redes de información, especialmente a internet.

3. Los metadatos son los datos que describen los registros generados respecto de los datos creados al utilizar las tecnologías de la información y comunicaciones.

4. En el caso de las llamadas telefónicas, los metadatos se generan por cada comunicación, son el rastro que perdura después de que se realizó una llamada a través de una línea, son un elemento muy valioso para las autoridades de justicia y seguridad nacional en la investigación de delitos.

5. Los metadatos de las comunicaciones realizadas por los usuarios de una línea, al estar asociados a los datos personales, comparten la cualidad de datos personales y requieren ser protegidos conforme a la ley, considerando el eslabón que los concesionarios ocupan en la cadena de valor de las TIC.

6. Las bases de datos de los concesionarios, creadas con propósitos de negocio, registran los metadatos de las comunicaciones de los usuarios, para facturar los consumos realizados.

7. La conservación y entrega de los metadatos a las autoridades competentes, obedece a un tratamiento establecido exprofeso en la ley, que se justifica en razones de seguridad pública de orden e interés públicos.

8. Las bases de datos creadas con propósitos de colaboración con la justicia, registran y conservan los metadatos, considerando el valor público de los metadatos en la investigación y persecución de delitos.

9. Los concesionarios son responsables del tratamiento de los metadatos conservados conforme al artículo 190, fracción II de la LFTR. El tratamiento de esta información personal está determinado por la ley y el cumplimiento de los principios se atiene por los concesionarios apegándose a la norma.

10. Si bien el tratamiento de los metadatos está definido por la LFTR, así como por los Lineamientos, el principio de responsabilidad corresponde cumplirlo principalmente a los concesionarios. Este principio se atiende, cumpliendo con los principios en materia de protección de datos personales y estableciendo al interior de la organización las medidas regulatorias adecuadas a la sensibilidad de los datos personales para protegerlos y brindarles seguridad.

11. El inventario de los metadatos es un paso necesario para poder identificar las medidas regulatorias de seguridad, que deben permitir, por lo menos, la confidencialidad, integridad y disponibilidad de los metadatos.

12. La cadena de valor del proceso de colaboración con la justicia, nos muestra la regulación en materia de protección de datos personales, así como el propósito que cumple cada eslabón hasta que dicha información sea cancelada.

13. El “Análisis de brecha” es el primer paso de un estudio de regulación de conformidad con LFPDPPP, que se aplica al sistema para generar las bases de datos de negocio preexistentes en la infraestructura del concesionario. El segundo paso, es aplicar la metodología de “Privacidad por diseño” antes de

la creación del sistema para conservar los metadatos y el proceso de entrega a las autoridades, y finalmente, el aspecto cíclico en la revisión orientada la mejora continua, consiste en el “Análisis de brecha periódico cada 12 meses” a todo el sistema utilizado para crear las bases de datos de regulación y el proceso de entrega.

14. En el cómputo en la nube, las bases de datos creadas y controladas por los concesionarios con propósitos de colaboración con la justicia, no pueden estar fuera del territorio nacional, ni ser objeto de consulta directa por autoridades extranjeras de seguridad y justicia.

15. El deber de "control" de los concesionarios también conlleva la responsabilidad de asegurarse, mediante la consulta a la ley y otras disposiciones aplicables, que el requerimiento de información provenga de una autoridad facultada y que la entrega de los metadatos requeridos se apegue a lo previsto en el artículo 190, fracción II de la LFTR, estableciendo las medidas para evitar entregar la información a otras autoridades no competente, o entregar cualquier información personal en poder del concesionario, que no esté prevista en la fracción en comento o en los Lineamientos.

16. Todas las medidas derivadas del análisis de brecha sobre las bases de datos de negocio, la metodología de privacidad por diseño, así como el análisis de brecha periódico que se realice al sistema de conservación y entrega de datos personales con propósitos de colaboración con la justicia, deben estar contenidas en un Plan de instrumentación y seguimiento.

17. Finalmente, los concesionarios están obligados a cumplir con el principio de información. Al efecto, deben indicar a los usuarios de servicios de telefonía, (i) cuáles son los metadatos que conservará en cumplimiento a la regulación, (ii) el hecho de que la conservación se realizará por cada comunicación

realizada por el usuario y (iii) que la conservación se realizará con el propósito de colaborar con la justicia indicando las autoridades competentes y la existencia del Plan de instrumentación y seguimiento.

Bibliografía

1. Libros y artículos especializados

ALLISON HOPE, Dunstan, “Protecting Human Rights in the Digital Age”, Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry, BSR, february 2011, Consultado el 22 de abril de 2017 en https://www.bsr.org/pdfs/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf

ÁLVAREZ, GONZÁLEZ DE CASTILLA, Clara Luz, “Internet y Derechos Fundamentales”, Porrúa, México 2011.

ÁLVAREZ, GONZÁLEZ DE CASTILLA, Clara Luz, “Derecho de las Telecomunicaciones” 2da, Libertad de expresión, Unam Posgrado, 2013, Puebla, México

AGENCIAS, “El escándalo da a conocer la escuela china sospechosa de los ciberataques a Google”, El país, 22 de febrero de 2010, consultado el día 10 de marzo de 2015 en http://tecnologia.elpais.com/tecnologia/2010/02/22/actualidad/1266832863_850215.html

AUSTRALIAN Government. Attorney-General´s Department. “Data Retention, Frequently Asked Questions for Industry”. Version 1.1 July 2015, Consultado el 22 de abril de 2017 en https://www.ag.gov.au/dataretention

BAILEY, Tucker, et al, “Playing war games to prepare for a cyberattack”, McKinsey Global Institute, Julio, 2012. . Consultado el día 27 de noviembre de 2014 en

http://www.mckinsey.com/insights/business_technology/playing_war_games_to_prepare_for_a_cyberattack

BRADLEY, Joseph, et al, “Internet of Everything (IoE) Top 10 Insights from Cisco’s IoE Value at Stake Analysis for the Public Sector”. Consultado el 27 de noviembre de 2015 en http://www.cisco.com/web/about/ac79/docs/IoE/IoE-VAS_Public-Sector_Top-10-Insights.pdf

CAVOUKIAN, Ann, “Privacy by Design, The Seven Fundational Principles”, consultado el dìa 22 de abril de 29017 en https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

CHINN David, et al, “Risk and responsibility in a hyperconnected world: Implications for enterprises”, McKinsey&Company, enero 2014., página 2. Archivo PDF consultado el 16 de diciembre de 2015 en http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises

TUPPEN, Chris, “Opening the Lines, A Call for Transparency from Governments and Telecommunications Companies”, Global Network Initiative, página 13, consultado el día 1 de septiembre de 2015 en https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf

GANTZ, John and REINSEL, David, “Extracting Value from Chaos”, Sponsored by EMC Corporation, junio 2011, consultado el 1 de febrero de 2015 en http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf

MANYIKA, James, et “Big data: The next frontier for innovation, competition, and productivity”, McKinsey & Company 2011.

NAVA GARCÉS, Alberto E., “Delitos Informáticos”, 2da, Porrúa, 2007, página 18.

OECD (2012), “The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy”, OECD Digital Economy Papers, No. 209, OECD Publishing. Consultado el día 31 de diciembre de 2014 en http://dx.doi.org/10.1787/5k8zq930xr5j-en

DIRECTRICES de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad, 2002. Consultadas el día 27 de noviembre de 2014 en http://www.oecd.org/internet/ieconomy/34912912.pdf

DECLARACIÓN de la CMSI+10 relativa a la aplicación de los resultados de la CMSI. Consultada el 27 de noviembre de 2014 en
http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/362828V2S.pdf

GUÍA para una evaluación de impacto en la protección de datos personales 2014 de la Agencia Española de Protección de datos personales, consultada el día 15 de noviembre de 2015 en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

GUÍA para implementar un Sistema de Gestión de Seguridad de Datos Personales, INAI, Noviembre 2014, Consultado el día 15 de noviembre de 2015 en http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementaci%C3%B3n_SGSDP_ene2014.pdf

ISO/IEC 27002:2005, Information Technology – Security techniques – Code of practice for security management. Citado por Kamruzzaman, Joarder et. al. “Security and Privacy in RFID Systems”, IGI Global Retrieved from www.knovel.com.

ISO/IEC 27001 Information technology -Security techniques - Information security management systems - Requirements

NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

PÉLISSIÉ DU RAUSAS Matthieu, et al, “Internet matters: The Next sweeping impact on growth, Jobs, and prosperity”, McKinsey Global Institute, mayo 2011. Consultado el 27 de noviembre de 2014 en http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters

PENTLAND, Alex, “Big Data: Balancing the Risks and Rewards of Data-Driven Public Policy”, The Global Information Technology Report 2014, Rewards and Risks of Big Data, World Economic Forum. Consultado el 22 de abril de 2017 en http://reports.weforum.org/global-information-technology-report-2014/

PRESTON, Alex, “The Death of Privacy”, The Guardian, 3 de Agosto 2014, consultado el 9 de marzo de 2015 en http://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

POZZI, Sandro. “Target despide al consejero delegado tras un ataque informático”, El País, 5 de mayo de 2014, consultado el 10 de marzo de 2015 en http://economia.elpais.com/economia/2014/05/05/actualidad/1399300492_653465.html

RUIZ, Bennett, et al, “The New Digital Economy. How it will transform business”, Oxfor Economics, Research paper produced in collaboration with AT&T, Cisco, Citi, PwC & SAP. June, 2011. Consultado el 22 de abril de 2017 http://www.pwc.com/mt/en/publications/the-new-digital-economy.html

ROBERTS, Dan y ACKERMAN, Spencer, “US intelligence outlines checks it says validate surveillance” The Guardian, consultado el 9 de marzo de 2015 en http://www.theguardian.com/world/2013/jun/16/nsa-the-nsa-files

WARREN, Samuel D. y BRANDEIS, Louis D., “The Right to Privacy”, Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890).

SPITZ, Malte, “Why Metadata Matters: The Dangers and Revealing Nature of Data Retention” consultado el 19 de febrero de 2015 en https://www.eff.org/node/81907

SOLÍS, Victor, “Datos de celulares a la Venta en Web”, El Universal, 3 de junio de 2010, consultado el 9 de marzo de 2015 en http://www.eluniversal.com.mx/notas/685120.html

TAUBERER, Joshua, “What is RFD”, Consultada el día 29 de Julio de 2014, http://www.xml.com/pub/a/2001/01/24/rdf.html.

The APEC Privacy Framework, Consultado el día 16 de febrero de 2015. http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

“Enduring Ideas, The Business System”, McKinsey and Company, consultado el día 27 de diciembre de 2015 en la siguiente liga http://www.mckinsey.com/spContent/Enduring%20IdeasV2/index.html#2513607397001?sid={12533493-15A2-4A46-8359-79C823E25C73}&pid={4386CABC-8926-43B7-B922-05933D401051}

OPINION 8/2014 on the on Recent Developments on the Internet of Things, página 7. Que fue consultada el 27 de noviembre en http://ec.europa.eu/justice/data-

protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

UIT Key ICT indicators for developed and developing countries and the world (totals and penetration rates), Consultado el 15 de diciembre de 2014 en http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

2. PÁGINAS DE INTERNET

http://es.wikipedia.org/wiki/Lenguaje_de_Control_de_Datos

http://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_base_de_datos

https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching

https://www.eff.org/node/81907

http://www.itu.int/wsis/implementation/2014/forum/inc/doc/outcome/362828V2S.pdf

https://www.eff.org/

3. REGULACIÓN

DICTAMEN sobre la Minuta de Proyecto de Decreto por el que se expide la Ley Federal de Telecomunicaciones y Radiodifusión.

LEY Federal de Telecomunicaciones y Radiodifusión.

ACUERDO mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y

modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996.

LEY Federal de Protección de Datos Personales en Posesión de los Particulares

PARÁMETROS de Autorregulación en materia de Protección de Datos Personales.

RECOMENDACIONES en materia de seguridad de datos personales.

4. CASOS DE LITIGIO

AMPARO EN REVISIÓN 937/2015, del índice de la Segunda Sala de la Suprema Corte de Justicia de la Nación. Consultado el día 10 de octubre de 2016 en http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=186831

TESIS 1A. CLV/2011, Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XXXIV, Agosto de 2011, página 221.